Introduction to Networking

Cybersecurity

Networking 101, Day 1

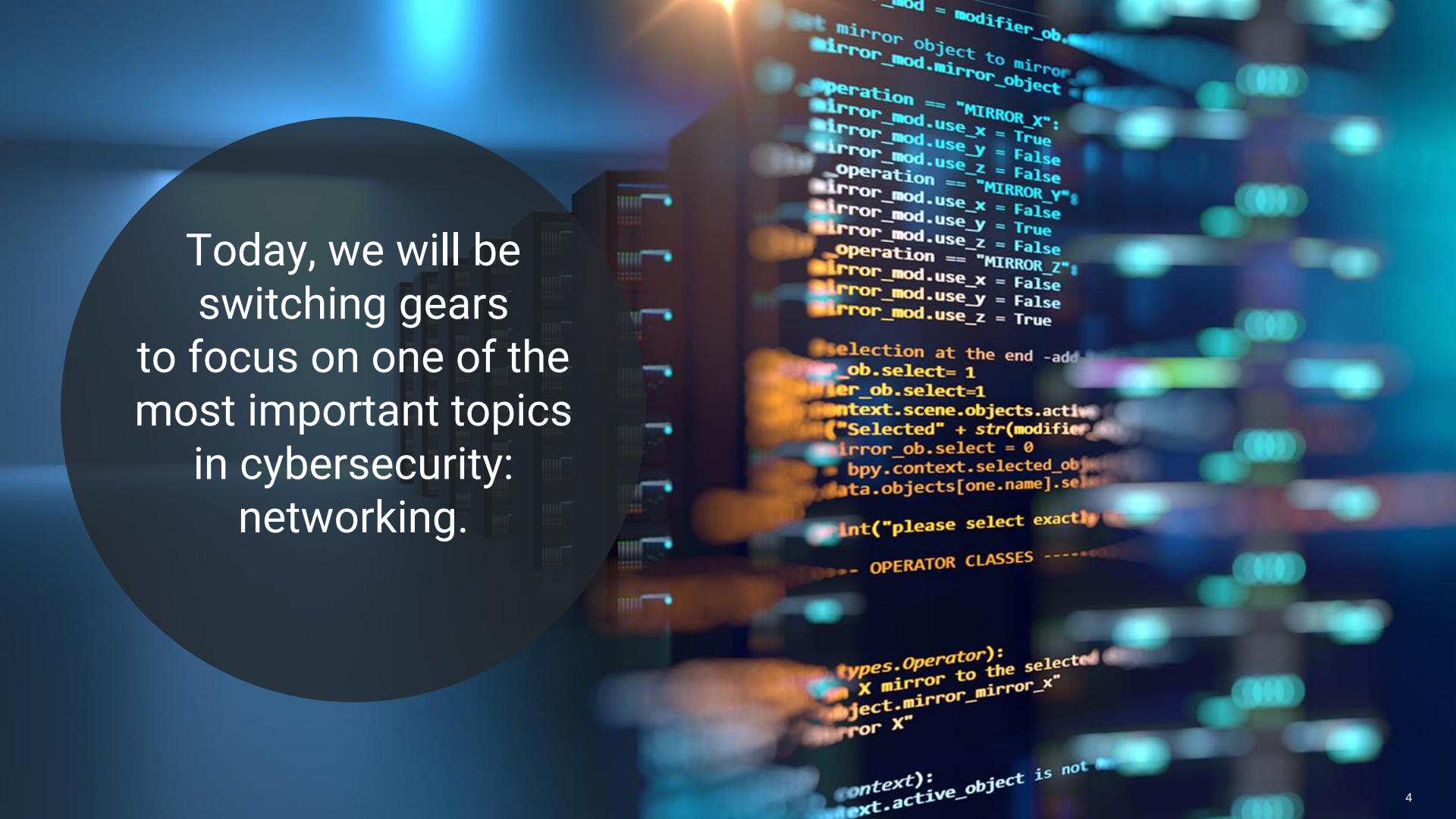
© 2019 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Class Objectives

By the end of today's class, you will be able to:

- Identify clients, servers, requests, and responses in network communications.
- Identify network topologies and compare their advantages and disadvantages.
- Design a conceptual network made of various network and network security devices.
- Convert binary numeric representations into readable IP addresses.
- Modify DNS host files to redirect the access of a website.

Introduction to Computer Networking


Today, we will be switching gears to focus on one of the most important topics in cybersecurity: networking.

Computer Networks

A computer network consists of multiple devices connected together to share resources and services.

Computer Networking

Knowledge of computer networking is essential for the following technical roles:

- **Security operations center (SOC) staff** commonly diagnose and troubleshoot network-related security issues and attacks. Understanding network devices and design can help them quickly resolve and identify these issues.
- **Network security engineers** are often involved in the design of a company's network architecture to protect their organization from security risks.
- **Penetration testers** test for vulnerabilities within a company's network. Understanding network design and common network vulnerabilities is core knowledge for penetration testers.

The Client-Server Model

Network Communication: The Client-Server Model

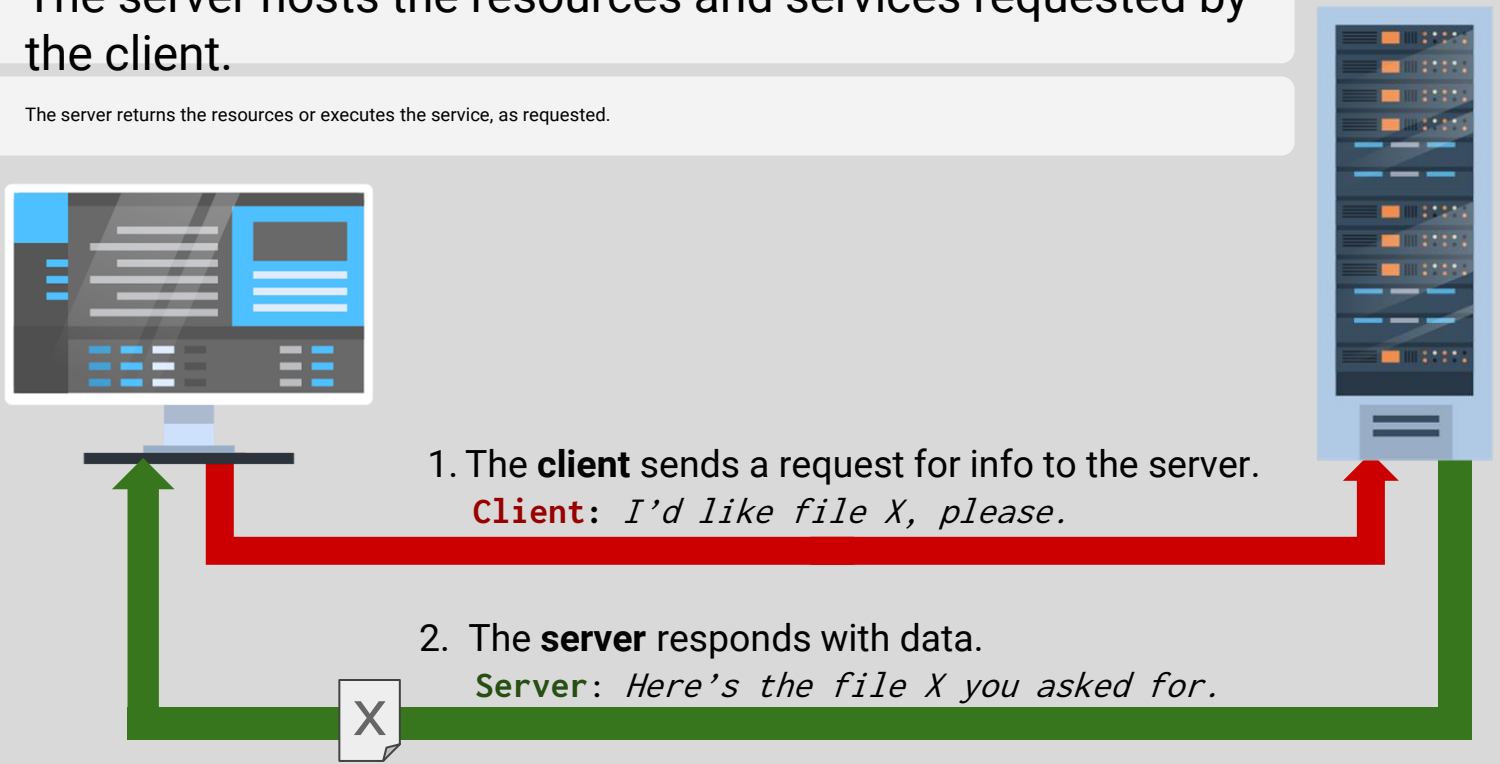
The **client-server model** is a network computing model that defines how resources and services are shared across a network.

Client-Server Model

The client is requesting a resource or a service.

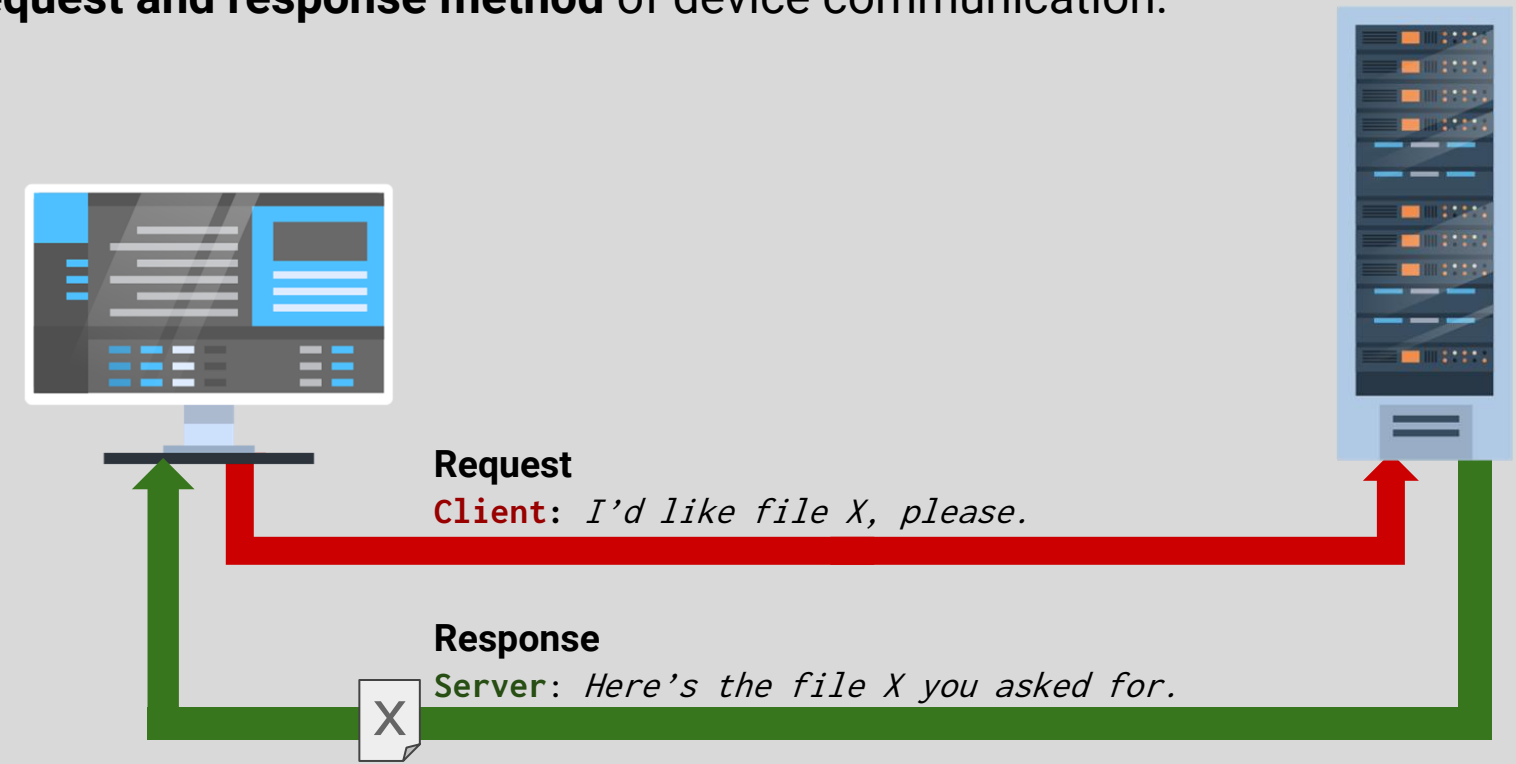
The server hosts the resources and services requested by the client.

The server returns the resources or executes the service, as requested.



Client-Server Model

This two-way conversation between the client and server is known as the **request and response method** of device communication.



Client-Server Model

01

The **request** is the process in which the client sends a message
to a server asking for a resource or to run
a service.

02

The **response** is sent back to the client after the server receives and processes the request.

03

The **response message** could be:

- An acknowledgement of the request.
- A requested resource.
- An error message.

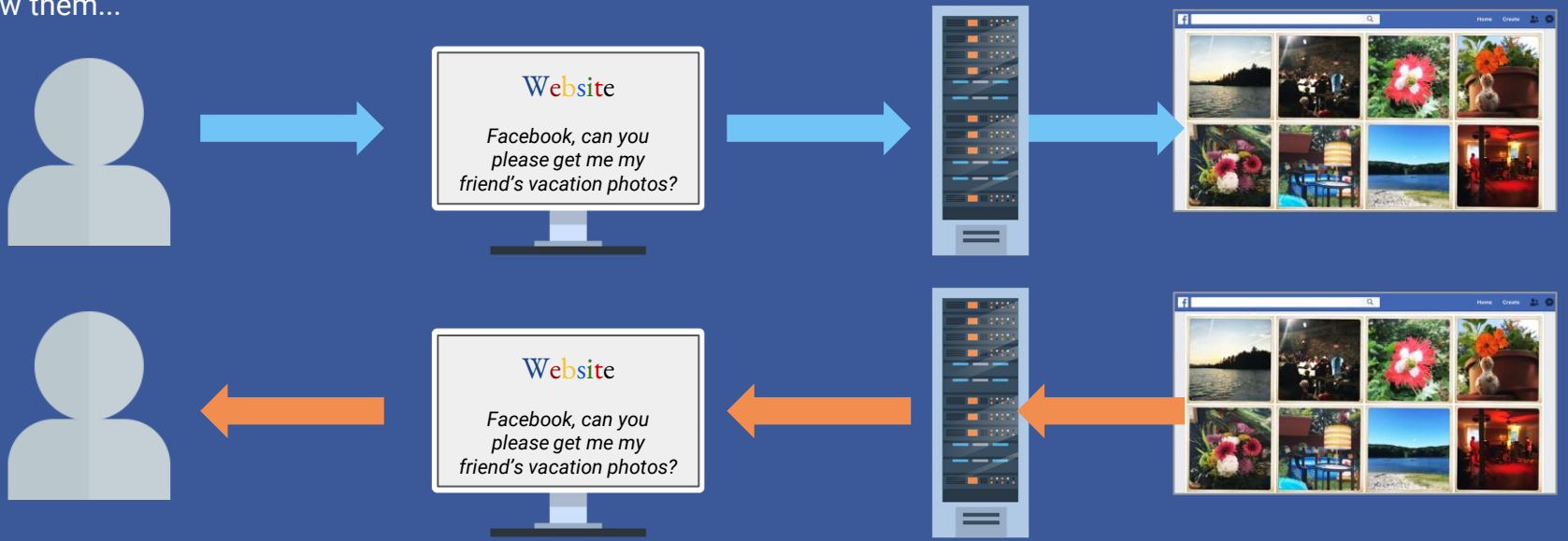
Client and Server Example

Let’s take the example of a webpage.

1. You want to view the vacation photos your friend posted on Facebook. When you view them...

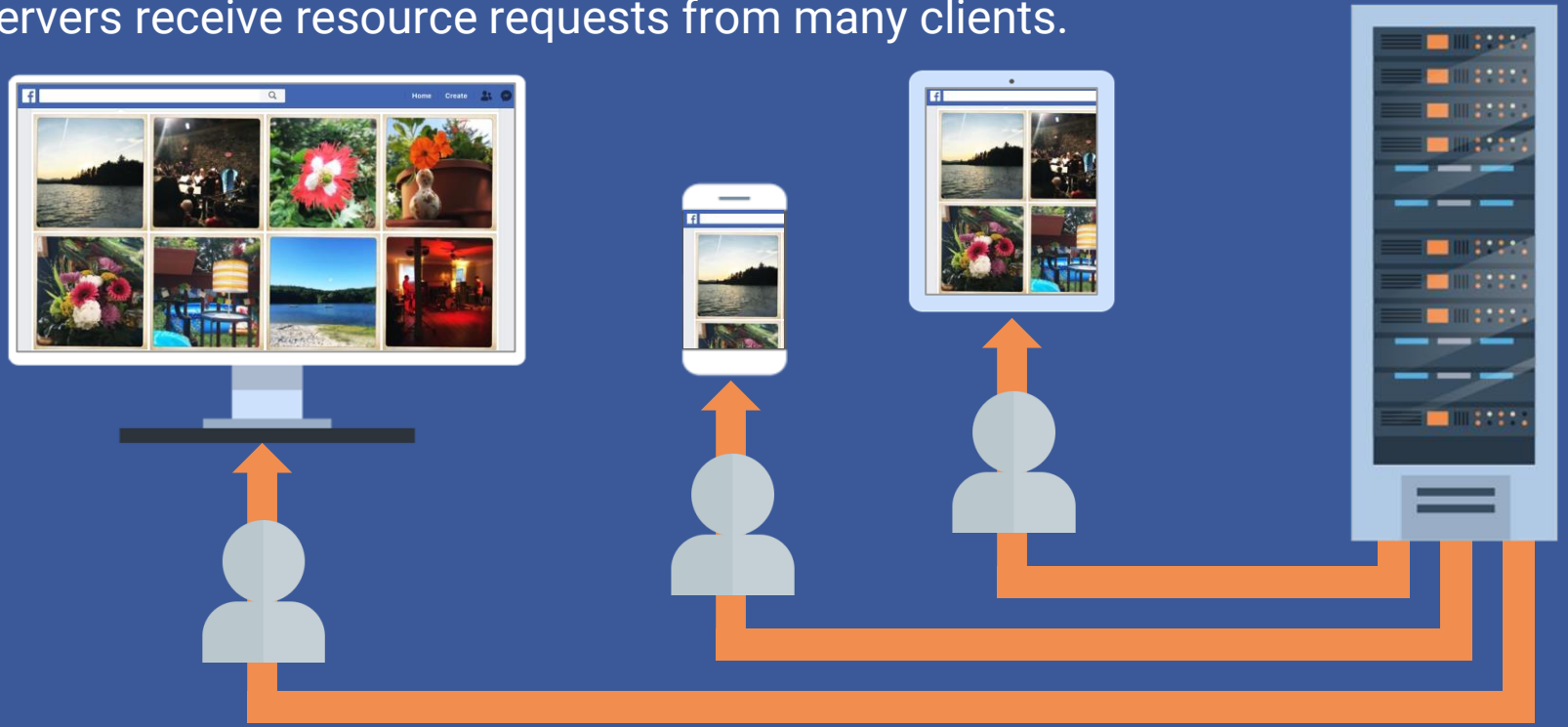
2. ...the browser is making a request: *“Facebook, can you please get me my friend’s vacation photos?”*

3. Facebook's web server provides a response: *“Yes, here are your friend's vacation photos.”*



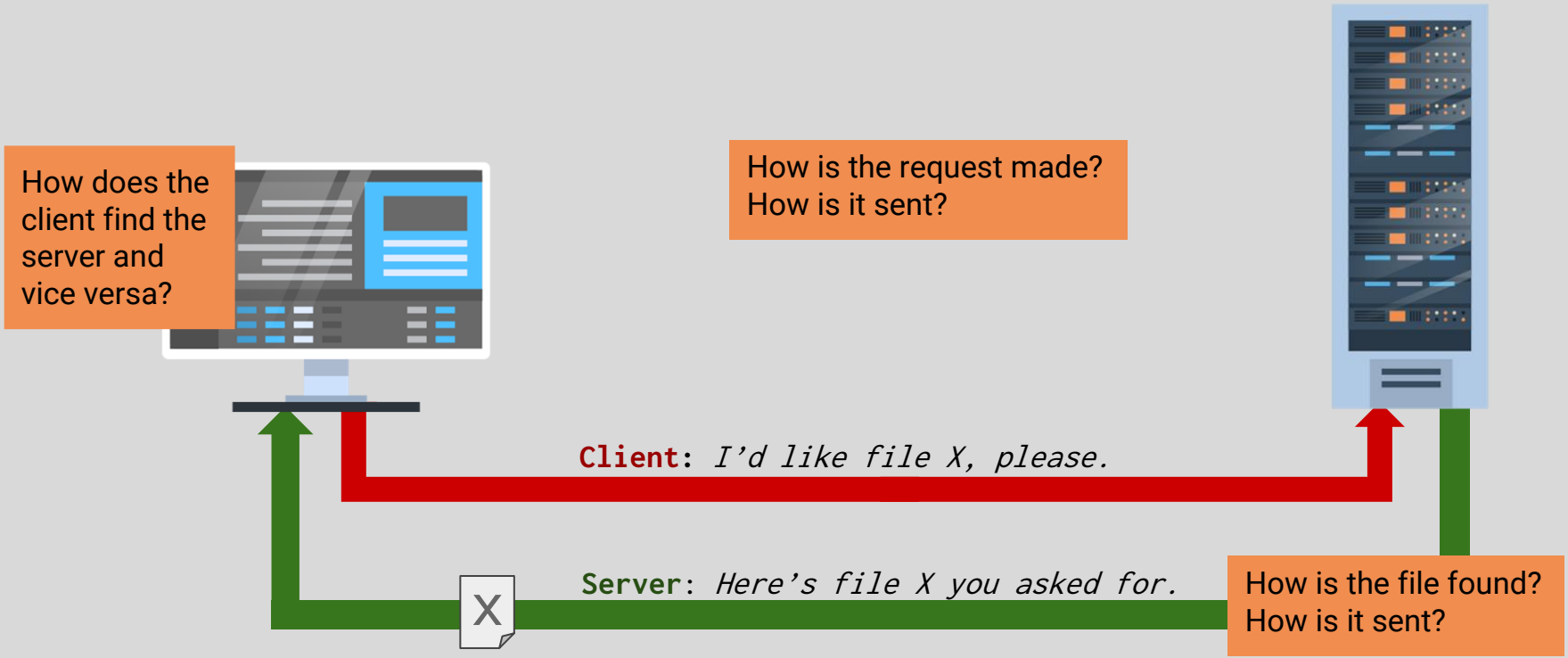
One Server, Many Clients

The client-server model is not a “one client, one server” relationship. Typically, servers receive resource requests from many clients.



Client-Server Model Continued

There's a lot to learn about this *"simple"* process.



Introduction to Network Security

Networks and Security

As we cover the tools and processes within the wide scope of networking, we will also discuss threats and risks.

Network security is the practices and policies used to protect and monitor a computer network's resources against these threats and risks.

Network Security

These risks and threats include:

- Unauthorized access to networks
- Denial of service (DoS) attacks
- Eavesdropping
- Datamodifcation

Activity: Network Security

In this activity, you will play the role of a security analyst at Acme Corp, which has recently experienced some suspicious activity on their systems.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Activity Review: Network Security

Scenario 1

A hacker logged into Microsoft Outlook with the stolen username and password of Acme's CFO. The hacker sent an email to the head of accounting asking them to wire $10,000 to a foreign account owned by the hacker.

Solution

- Client: Microsoft Outlook.
- Server: Email server or the mail exchange server.
- Request: Send the email.
- Response: Confirmation from exchange server that the email is received.

Review continued on next slide.

Activity Review: Network Security

Scenario 2

A hacker used Firefox to visit the administrative website of Acme Corp, where they attempted to log into the CFO's account multiple times, until they correctly guessed the password.

Solution

- Client: The browser, Mozilla Firefox.
- Server: The web server hosting the administrative webpage.
- Request: Attempt to log into the admin site.
- Response: Login attempt is accepted or denied.

Review continued on next slide.

Activity Review: Network Security

Scenario 3

A hacker stole the Acme CFO's mobile phone. Login credentials were saved on the phone, allowing the hacker to log into Acme Corp's mobile admin application.

Solution

- Client: The mobile admin app on the mobile phone.
- Server: Web application hosting the data, which the app is pulling from.
- Request: Attempt to log into the mobile admin application.
- Response: Login attempt is accepted or denied.

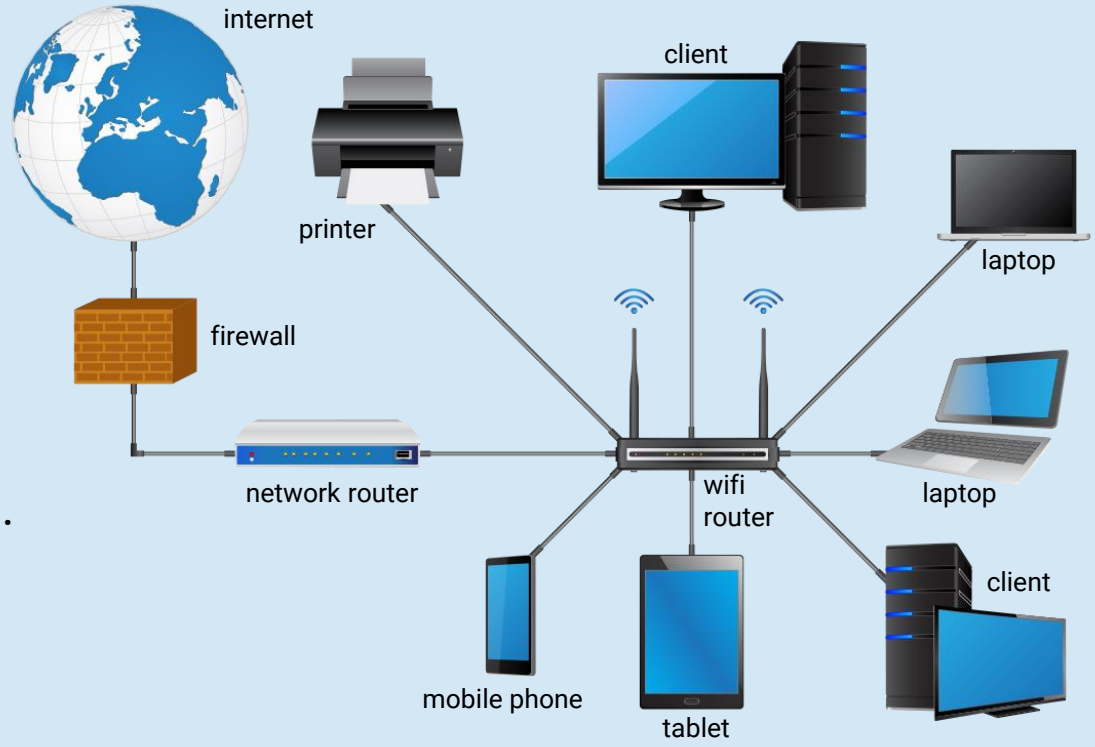
Network Structure

As mentioned, a computer network consists of multiple devices (nodes) connected to each other. **But how exactly are they connected?**

Local Area Network

When computer networks were first created, they were smaller private networks designed to connect devices within the same room or building.

This type of network is a **local area network (LAN)**—a private computer network that connects devices in smaller physical areas.



Benefits of LANs

LANs offer the following advantages:

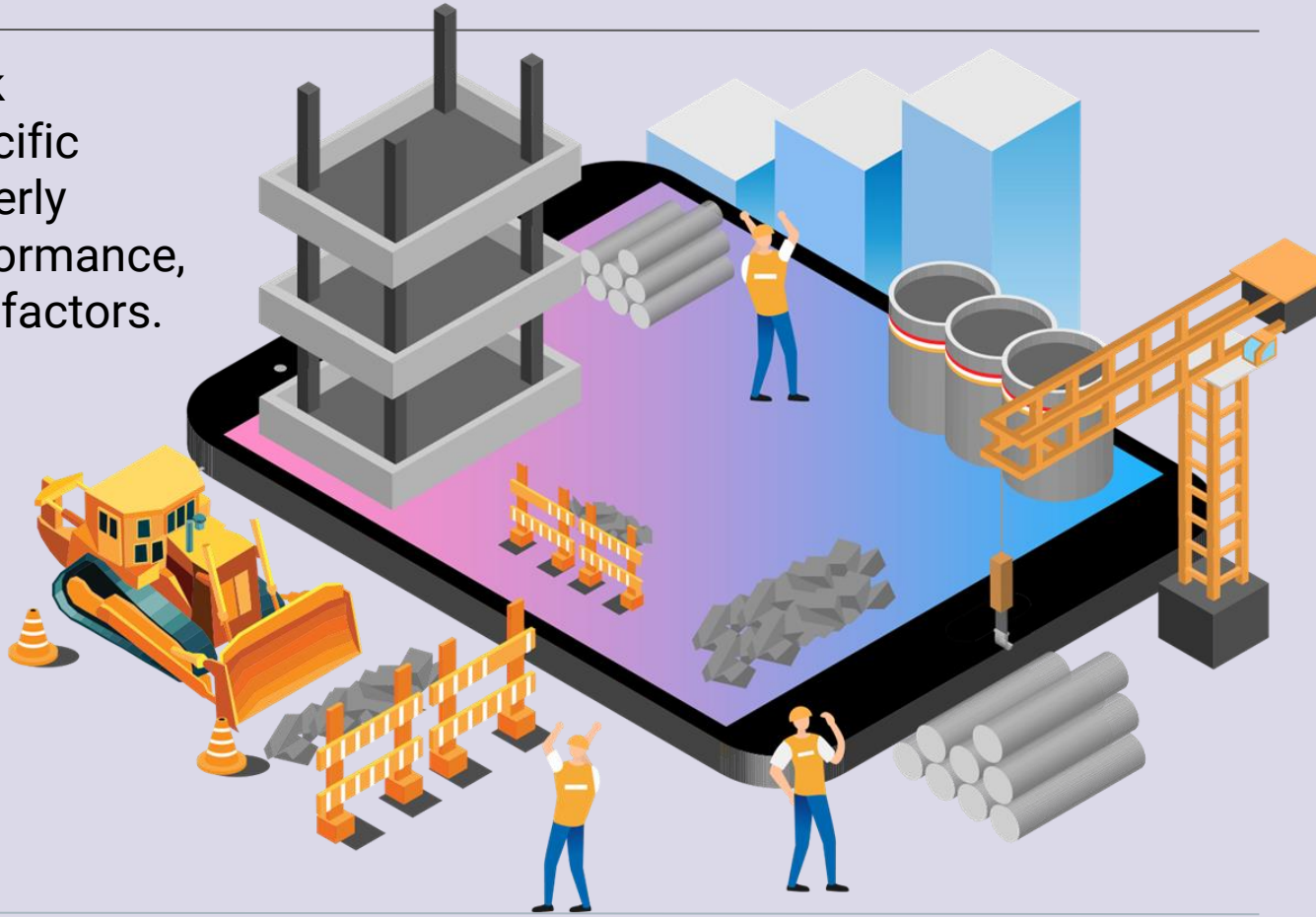
- Network speed and performance: Since the devices are physically near each other, connections are significanly faster and perform better.
- Network security: With security devices, a business can control what data comes in and out of their local network as well as who has access to resources.
- Versatility: New network devices can be easily added or removed inside a LAN due to the proximity of the devices within the network.

As technology advanced, computer networks expanded and small networks in different locations were able to connect, creating **Wide Area Networks (WAN)**.

Network Topologies

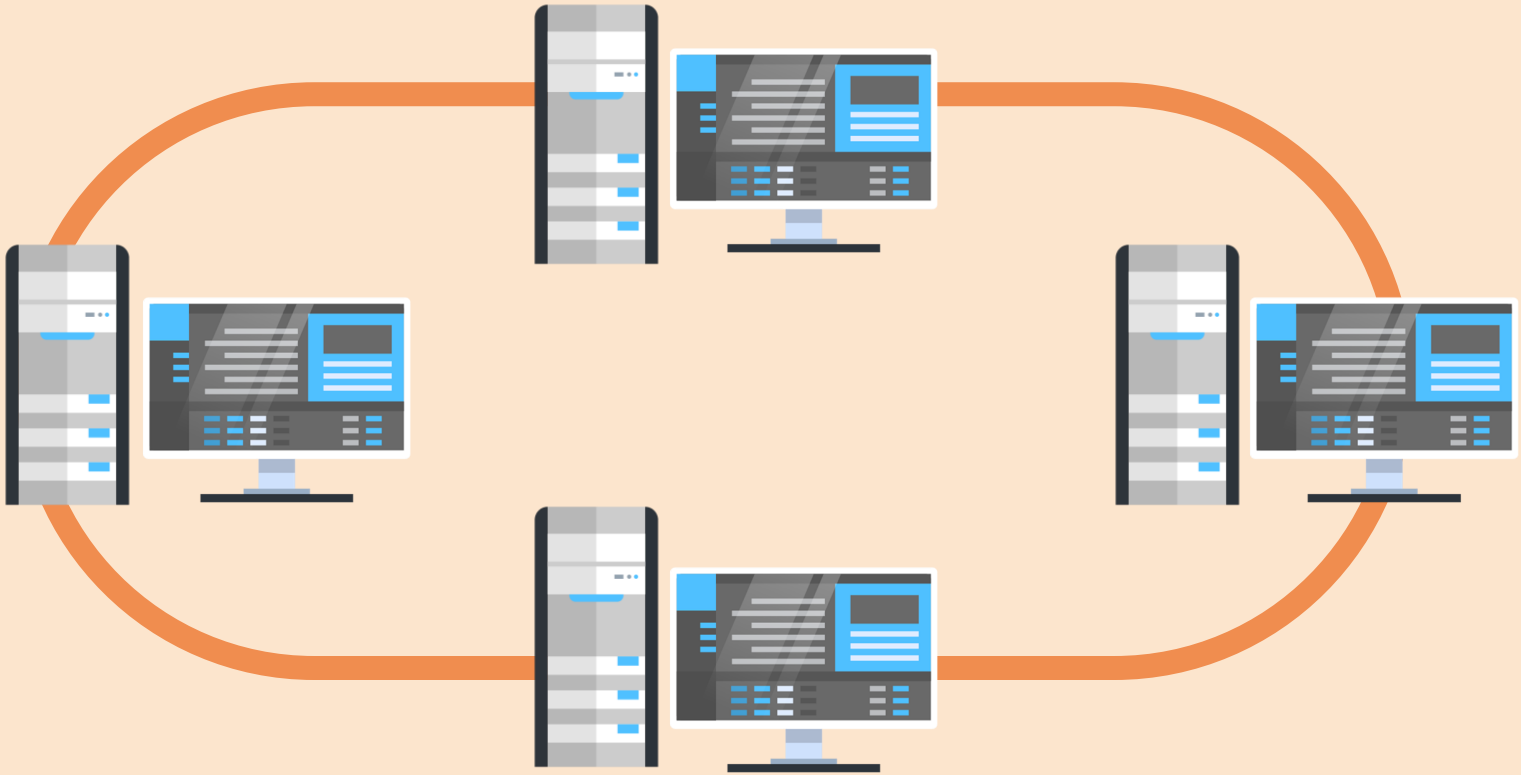
Machines on a network are connected in a specific design in order to properly serve the required performance, data flow, and security factors.

There are a variety of network topologies. These are named for the geometric shape of their design.



Network Topologies

Ring



Network Topologies

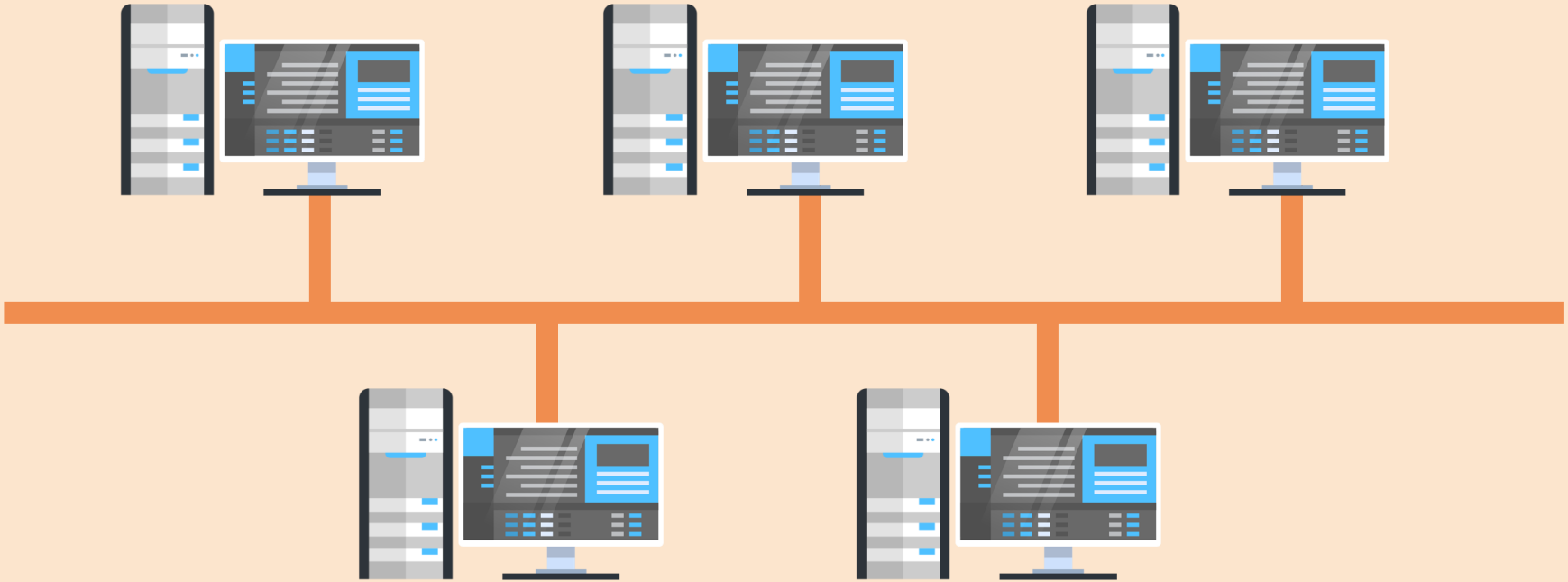
Linear

Network Topologies

Star

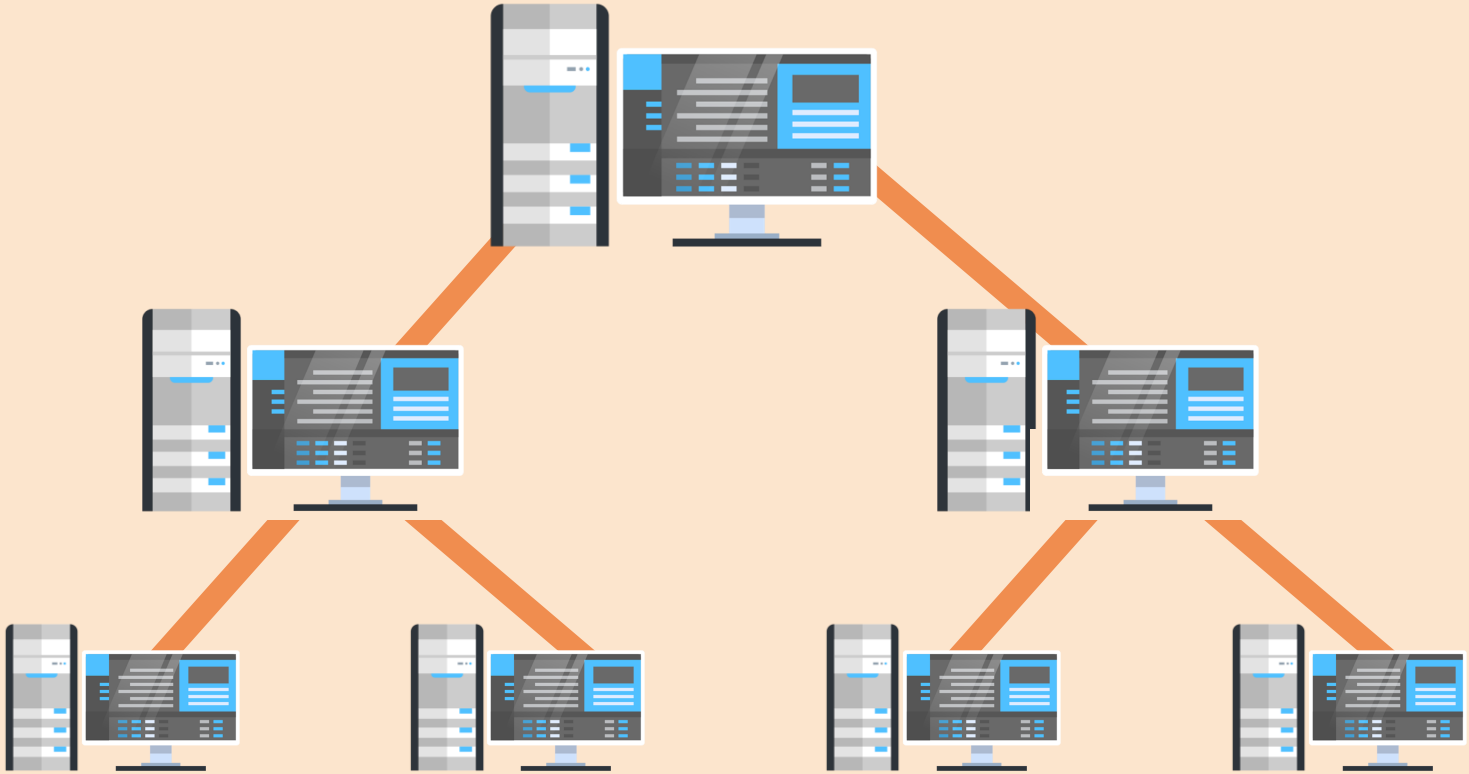
Network Topologies

Bus



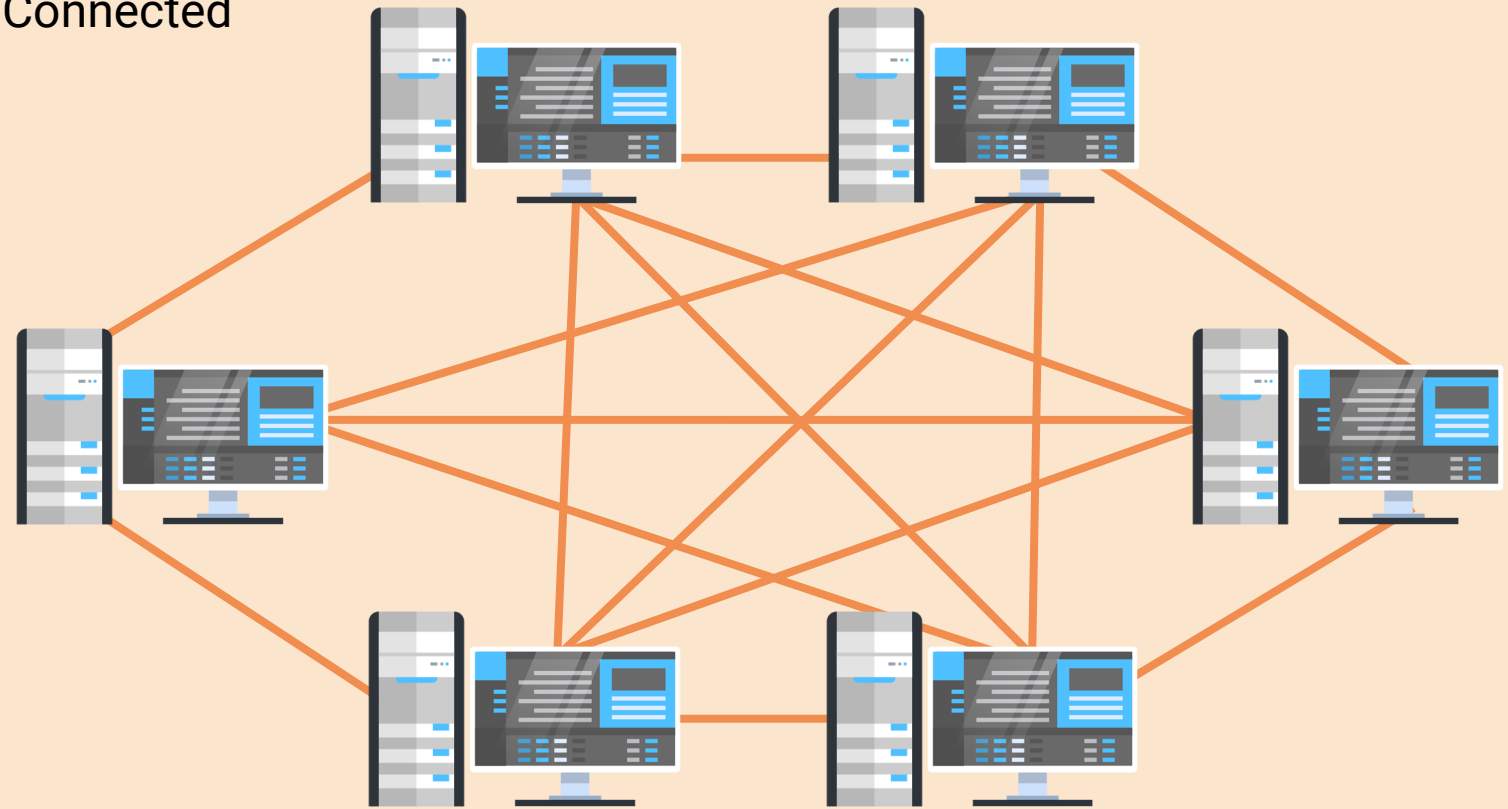
Network Topologies

Tree



Network Topologies

Fully Connected

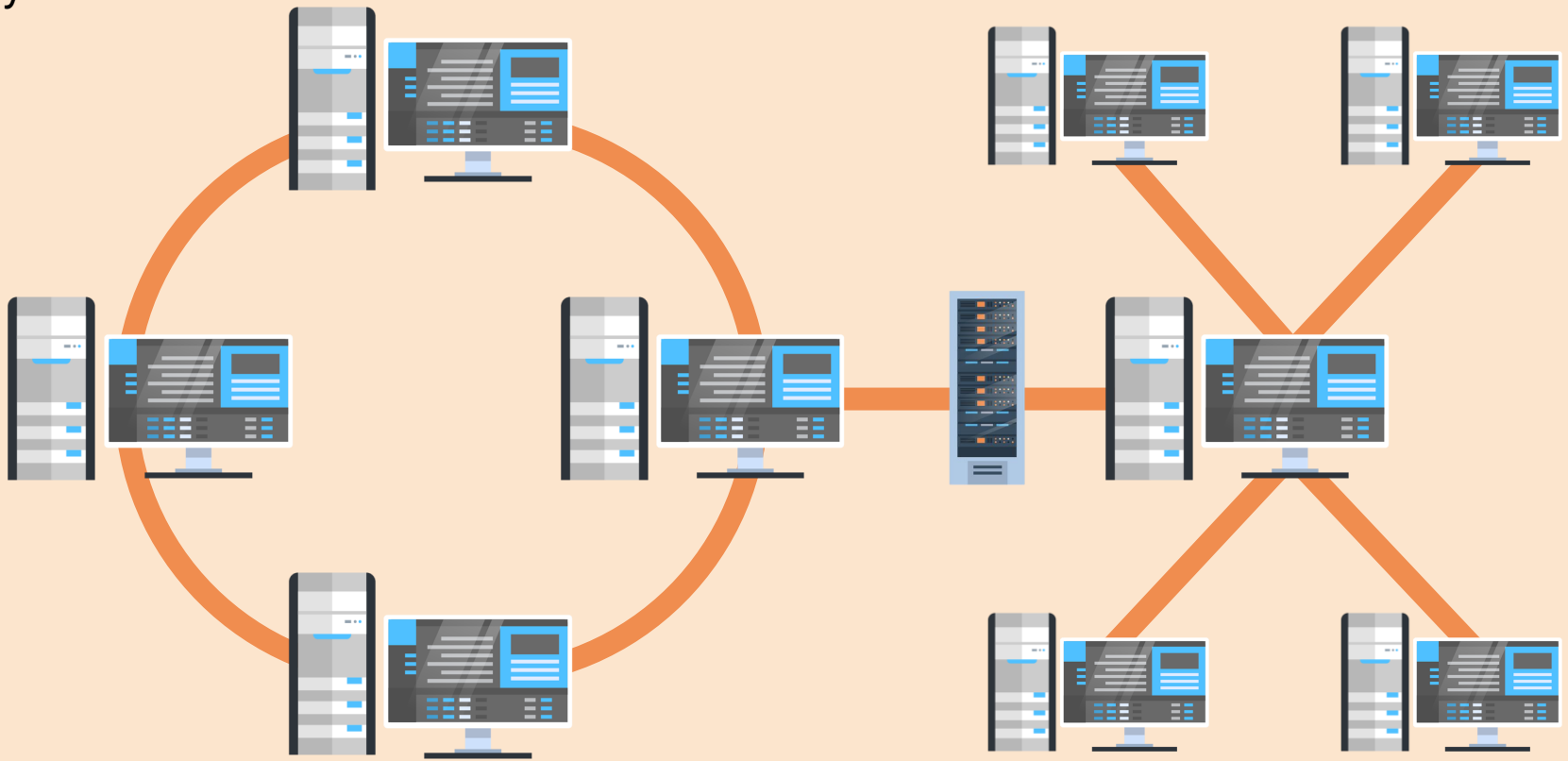


Network Topologies

Mesh

Network Topologies

Hybrid



Topologies and Network Security

If an attacker takes down a device that is a “point of failure,” that local area network will be impacted.

Activity: Network Structure

In this activity, you will continue to play the role of a security analysts at Acme Corp. You will review network diagrams to determine a hacker’s potential impact to the various office networks.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Activity Review: Network Structure

Sydney Office

Topology: **Ring**

- If the hacker disrupts the network traffic from the assumed location, the whole office will be impacted. In ring topologies, all the traffic flows in one direction. One device that loses connectivity impacts all the other devices.
- No matter which device the hacker is at, the entire Sydney office will go down if the hacker takes down their device's network.

Review continued on next slide.

Activity Review: Network Structure

Paris Office

Topology: **Star**

- If the hacker disrupts the network traffic from the assumed location, only the hacker's device will be impacted. The office's network will still work because the central device connecting all the other devices is still operational.
- The only device that would have a large impact is the central node of the star, which would take down the whole office if the hacker disrupted the network traffic.

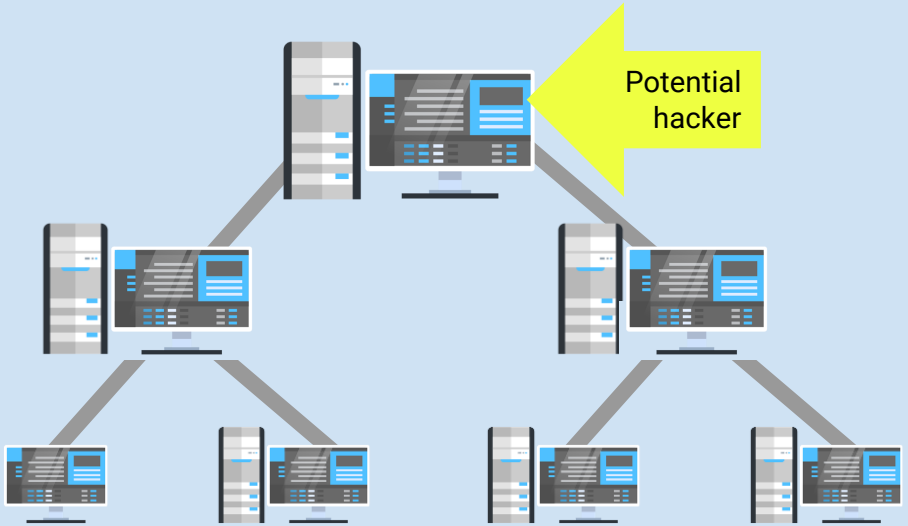
Review continued on next slide.

Activity Review: Network Structure

Bogotá Office

Topology: **Tree**

- If the hacker disrupts the network traffic from their assumed location, the whole office will be impacted because the hacker is the top node in the tree.
- If the hacker disrupted the network traffic from a device below the indicated location, it would only impact the devices falling below them. If there are no devices below, only the hacker's device would be impacted.



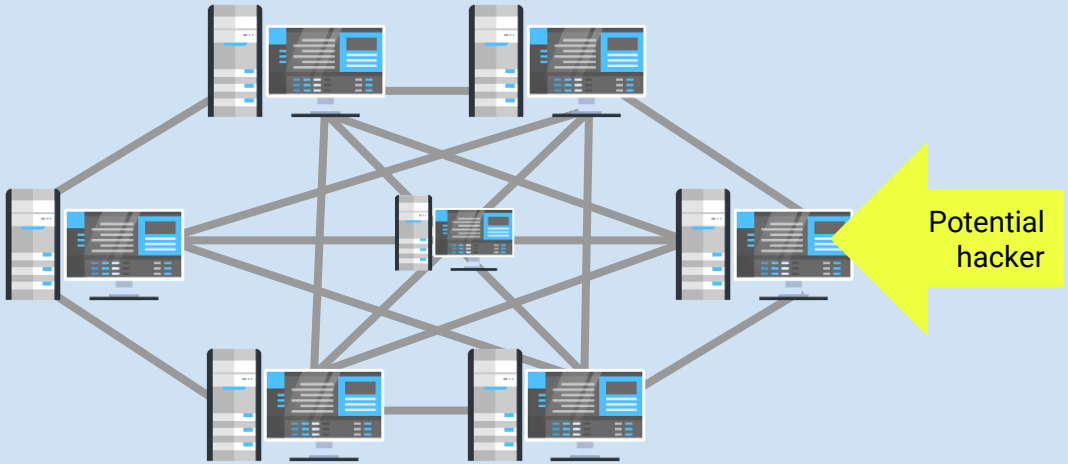
Review continued on next slide.

Activity Review: Network Structure

San Diego Office

Topology: **Mesh**

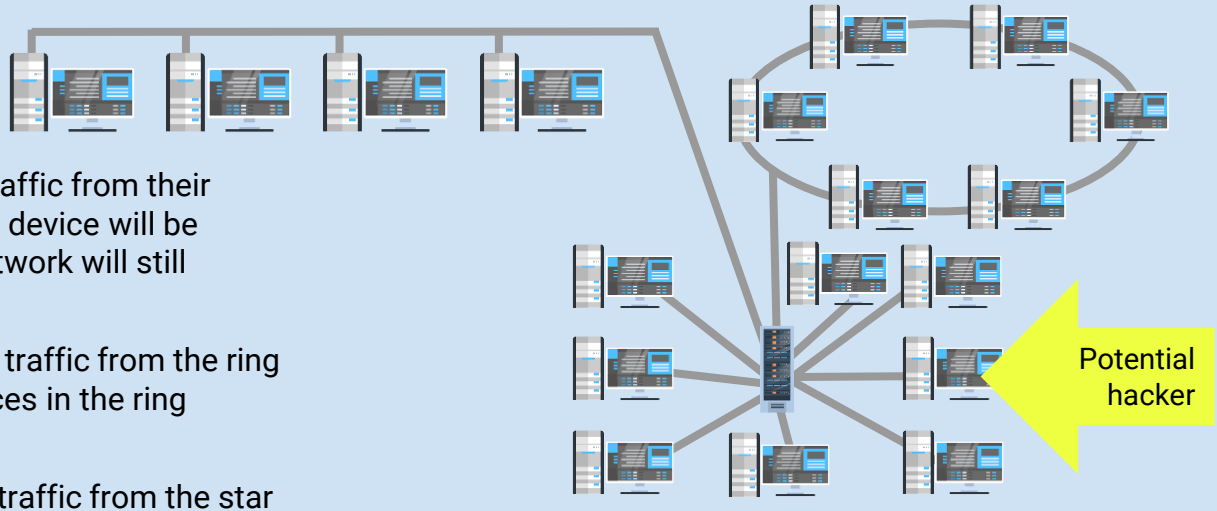
- If the hacker disrupts the network traffic from their location, only the hacker's device will be impacted. The office's network will still work, as each device has another connection to the others.
- If the hacker disrupted the network traffic from any other device, only the hacker's device would be impacted. The office's network would still work as each device has another connection to each other.



Review continued on next slide.

Activity Review: Network Structure

Tokyo Office

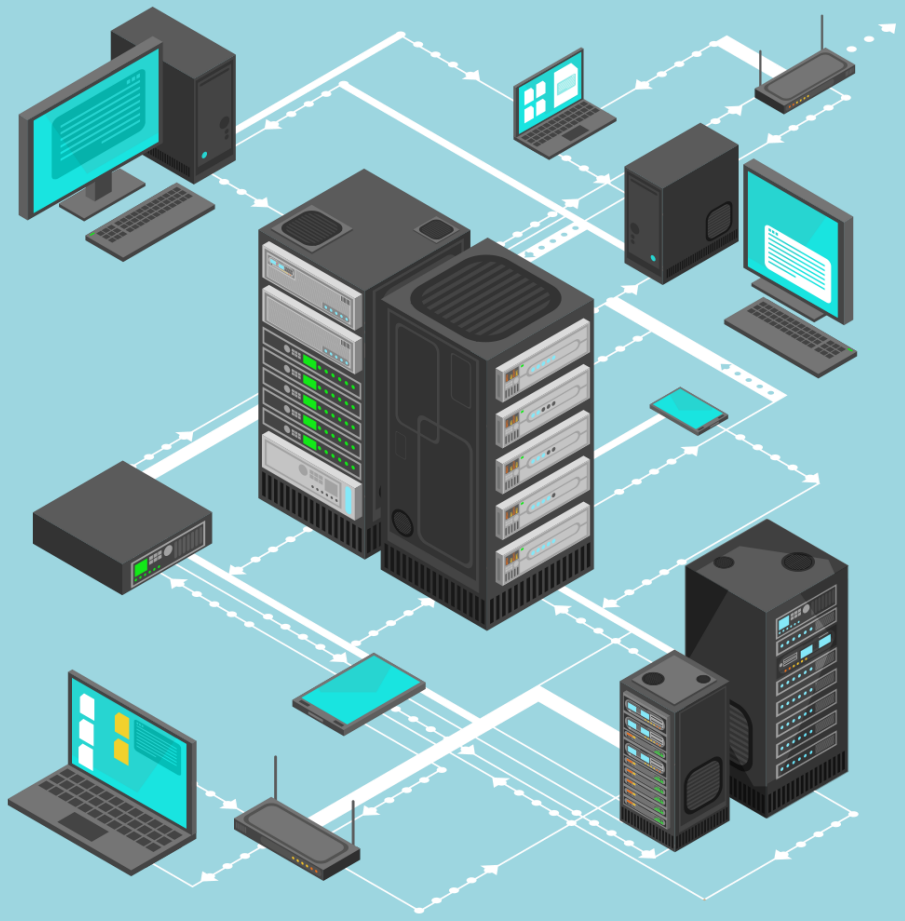


Topology: **Hybrid**

- If the hacker disrupts the network traffic from their assumed location, only the hacker's device will be impacted. The office's complete network will still function.
- If the hacker disrupted the network traffic from the ring section of the topology, all the devices in the ring topology would be affected.
- If the hacker disrupted the network traffic from the star section of the topology (not including the center device), only the device disrupted will be affected.
- If the hacker disrupted the network traffic from the bus section of the topology, all the devices could lose some form of connectivity depending where the traffic originates from.

Network Devices

The nodes that connect a network are actually many different devices, each with a variety of responsibilities.



Network Devices: Router

A **router** is a networking device that forwards (routes) resources to other networks. A router can connect two different LANs, two different WANs, a LAN to a WAN.

Routers are commonly used to connect a home network (a LAN) to the internet (a WAN).

Router Symbol

Network Devices: Switch

A **switch** is a networking device that forwards resources within a network. In other words, switches connect devices within a LAN.

Switches are typically used in large businesses with many computers.

Switches typically feed into routers.

Switches are intelligent devices, meaning they can be programmed to direct resources to certain computers.

Switch Symbol

Network Devices: Hub

A **hub** serves the exact same purpose as a switch, except it is not an intelligent device. Therefore, hubs cannot be programmed. Instead, they will direct a copy of the exact same resource to all computers connected to them.

Hubs are less secure than switches since they direct resources to all computers, even those that do not need them.

Hubs are outdated and no longer commonly used.

Hub Symbol

Network Devices: Bridge

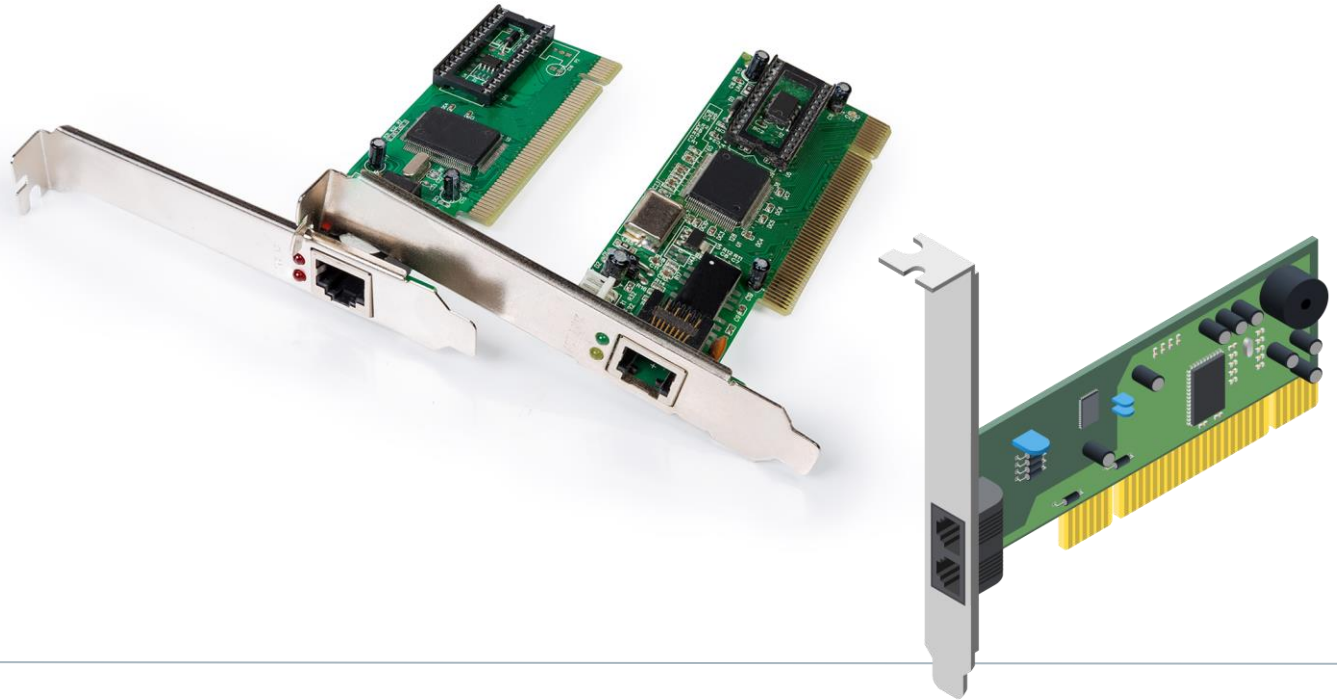
Bridges are switches that only have two connections: one in and one out.

Bridges are often used to tie two LANs together.

Bridge Symbol

Network Devices: Network Interface Controller (NIC)

An **NIC** is hardware that connects a computer to a computer network.



An **NIC** is usually a circuit board or chip installed on a computer.

Each computer must have an NIC in order to receive or send resources.

NICs can be wired or wireless.

NIC Symbol

Network Devices: Modem

Modems (*modulator-demodulator*) converts resource data into a format that the next type of connection can understand.

In simple terms: your computer and your internet service provider speak different languages, and the modem acts as the translator.

Your computer speaks "digital" and your ISP speaks "analog."

A **modem** translates between your computer and the ISP so they can understand each other.

Modem Symbol

Network Devices: Wireless Access Point (WAP)

WAPs allow wireless devices to connect to a wired network.

Network Devices: All-in-One Device

All-in-one devices can have modems, WAPs, routers, and more all built into a single device. All-in-one devices are very common household devices.

The advantage of **all-in-one devices** is ease of use, as less equipment needs to be set up and maintained.

The disadvantage is that they're a single point of failure, and difficult to troubleshoot.

Router Symbol

The previous devices work to transfer data across networks.

There are also network security devices used to protect resources on the network.

Network Security Devices: Firewall

A **firewall** is an intelligent network security device that monitors incoming and outgoing traffic based on security rules.

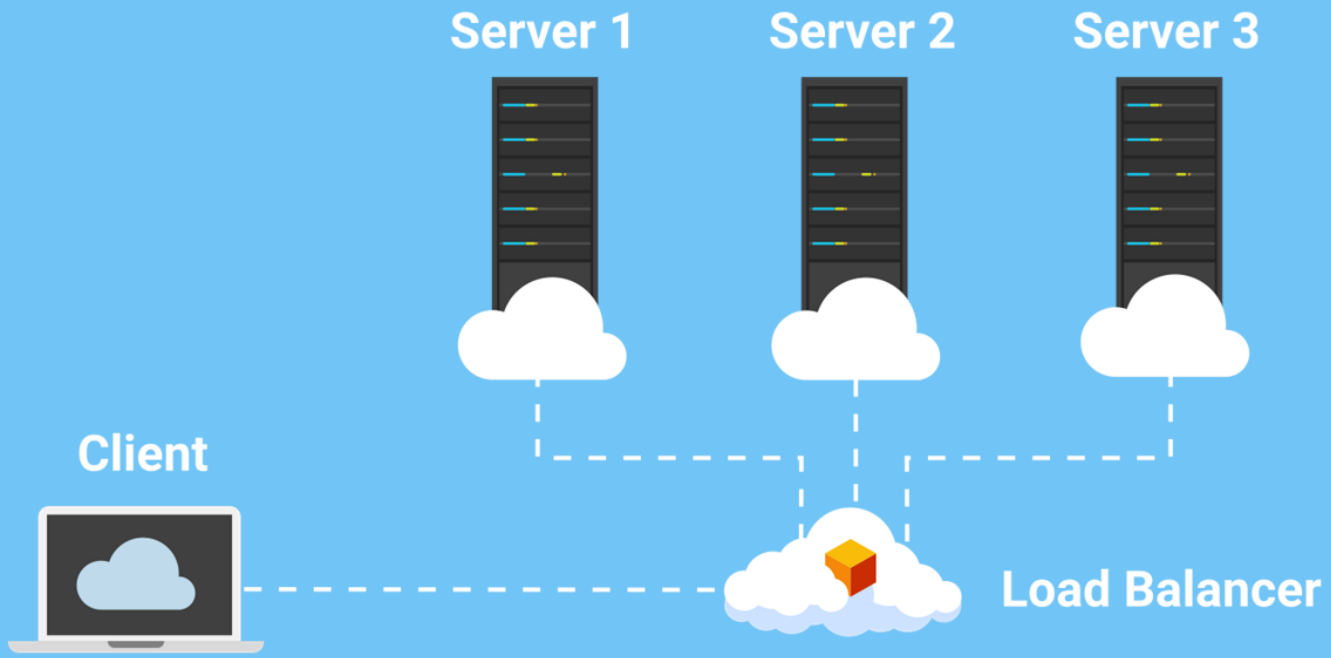
Firewalls are typically placed at the entry point of a LAN. This protects the resources inside.

There are many types of firewalls and specific firewall functionalities—these will be covered In future lessons.

Firewall Symbol

Network Security Devices: Load Balancers

A **load balancer** is an intelligent network security device that distributes incoming network traffic across multiple servers.



A **load balancer** ensures no single server has too much traffic to handle.

Load balancers help protect the availability of resources.

For example: If a server receives more resource requests than it can handle, it may go down or fail to handle a resource request.

Network Security Devices: Demilitarized Zones (DMZ)

A **DMZ** is a smaller subnetwork within a LAN used to add an additional layer of security to an organization's LAN, protecting secure data within the internal networks.

A **DMZ** typically has its own network security devices, such as firewalls, that attempt to detect network attacks before they access the internal networks.

A common task for network and security professionals is to visually design a setup before purchasing, installing, and configuring a network with these devices.

Network Design Demo

Designing your network visually can assist with the following:

01

Making networks more efficient, since proximity of certain devices can reduce latency.

02

Avoiding the creation of a "single point of failure."

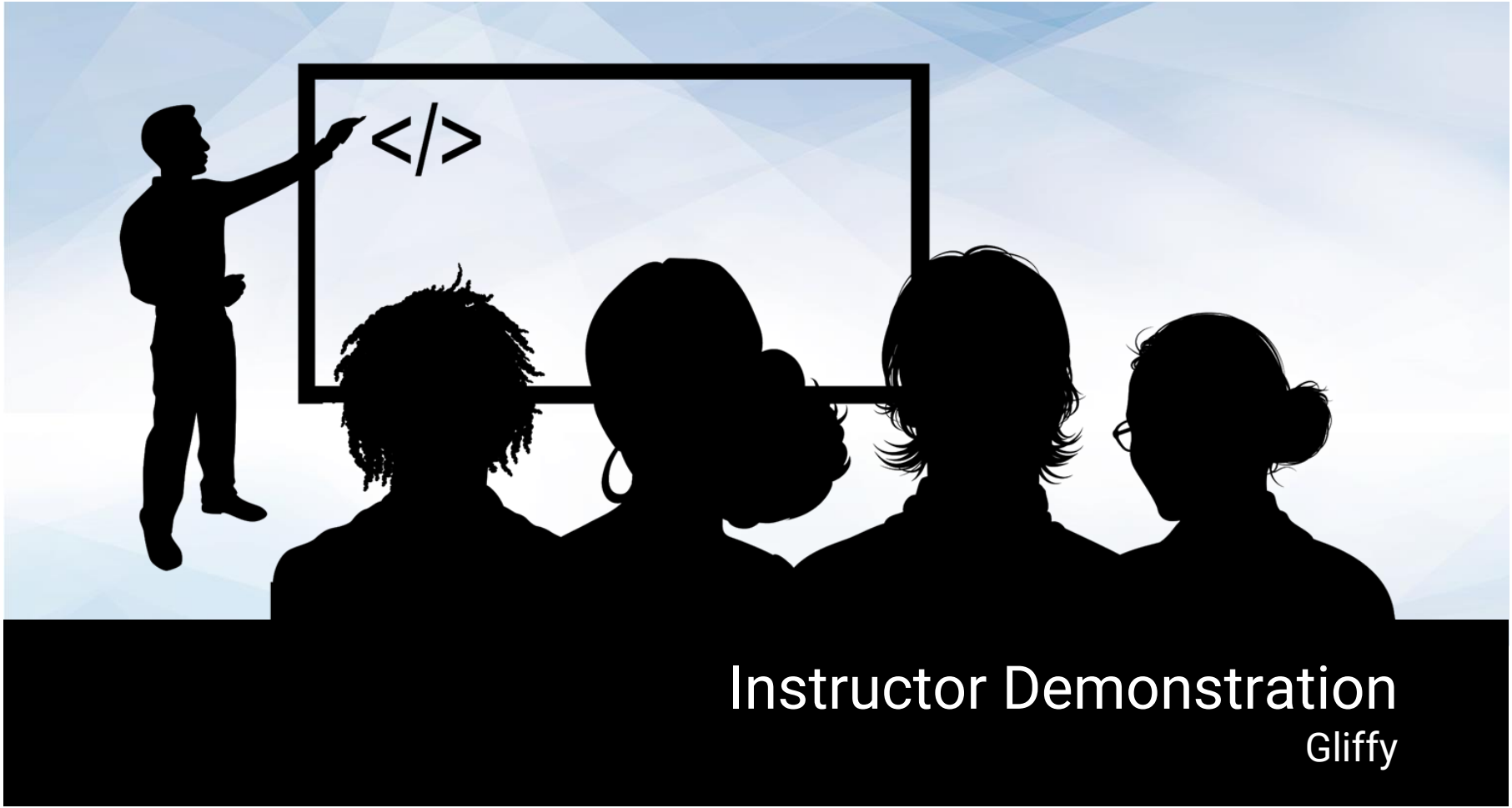
03

Ensuring private resources are protected from unauthorized sources.

Network Design Demo

In the next demo, we will use the free web tool Gliffy to design a basic network incorporating the following devices:

- 2 Computers
- 1 Switch
- 1 Router
- 1 Firewall
- 1 Representation of the internet



Instructor Demonstration

Gliffy

Activity: Network Devices

In this activity, you will continue to play the role of a security analyst at Acme Corp. You will design a network layout for the Shanghai office using Gliffy.

You will also need to add network security devices to the design to protect against a network attack.

Suggested Time:
20 Minutes

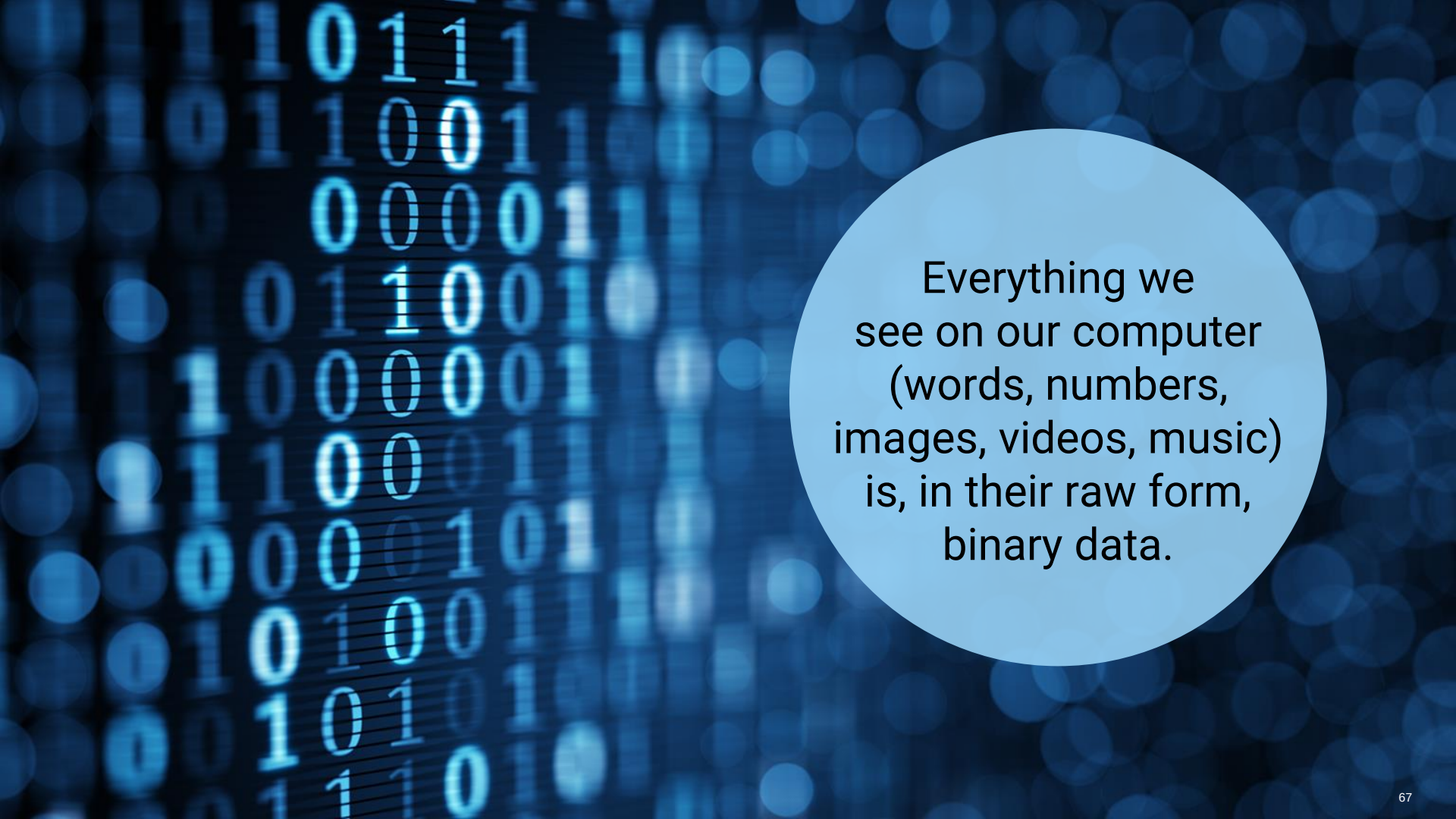
Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

“What’s My Address?”
Binary Data and IP Addresses



Everything we see on our computer (words, numbers, images, videos, music) is, in their raw form, binary data.

Binary Data

At the most basic level, computers communicate with electric signals, which have two states: **on** and **off**.

Binary is the two-digit numerical system that indicates if a signal is on or off.

Visualized, these on and off signals are depicted as ones and zeros.

1 = On

0 = Off

Meaning is created through the specific and repeated triggering of these **on** and **off** signals. This binary data is eventually transformed into the data we see on our devices.

Binary Data

Our computer wants to transmit 1 2 3 4 5.
It would transmit this message using binary data:

1 = `00000001`

2 = `00000010`

3 = `00000011`

4 = `00000100`

5 = `00000101`

This data would then be converted into the human-readable string: 1 2 3 4 5.

Binary vs. ASCII vs. Decimal vs. Hexadecimal

Binary is one of many alphanumeric representations of data. A few others:

Binary

Two-digit numerical system using 0 and 1.

```
01000001 00101100 00100000
01000010 00101100 00100000
01000011 00101110 00001010
01001001 01110100 10000000
011001   01110011 00100000
01100101 01100001 01110011
01111001 00100000 01100001
01110011 00100000 00001010
00110001 00101100 00100000
00110010 00101100 00100000
00110011 00100001 00100000
00001010
```

Decimal

Ten-digit numerical system using 0–9.

65 44 32 66 44 32
67 46 10 73 116
8217 115 32 101
97 115 121 32 97
115 32 10 49 44
32 50 44 32 51 33
32 10

Hexadecimal

Sixteen-digit alphanumerical system.

41 2c 20 42 2c 20
43 2e 0a 49 74
2019 73 20 65 61
73 79 20 61 73 20
0a 31 2c 20 32 2c
20 33 21 20 0a

ASCII

All the numbers, letters, and special symbols we are familiar with.

A, B, C.

It's easy as

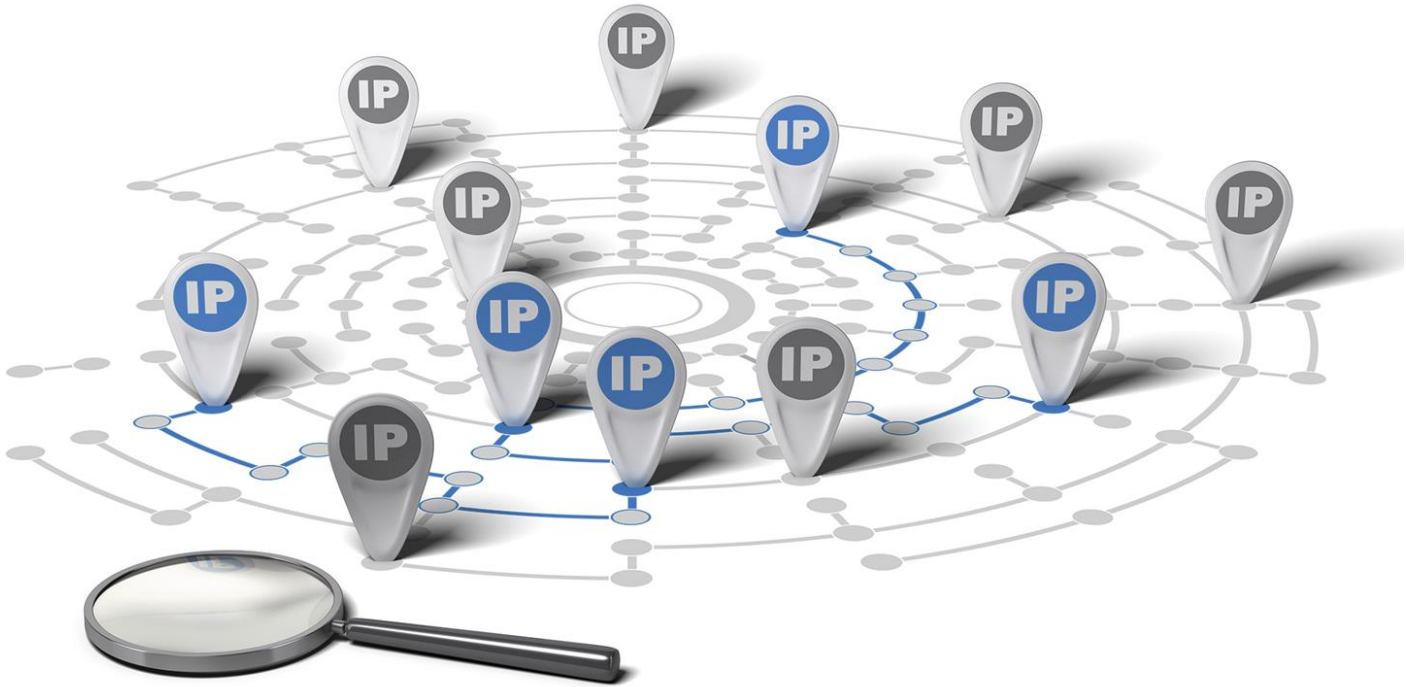
1, 2, 3!

Binary data is used for indicating the network addresses that machines need to direct and deliver data across networks.

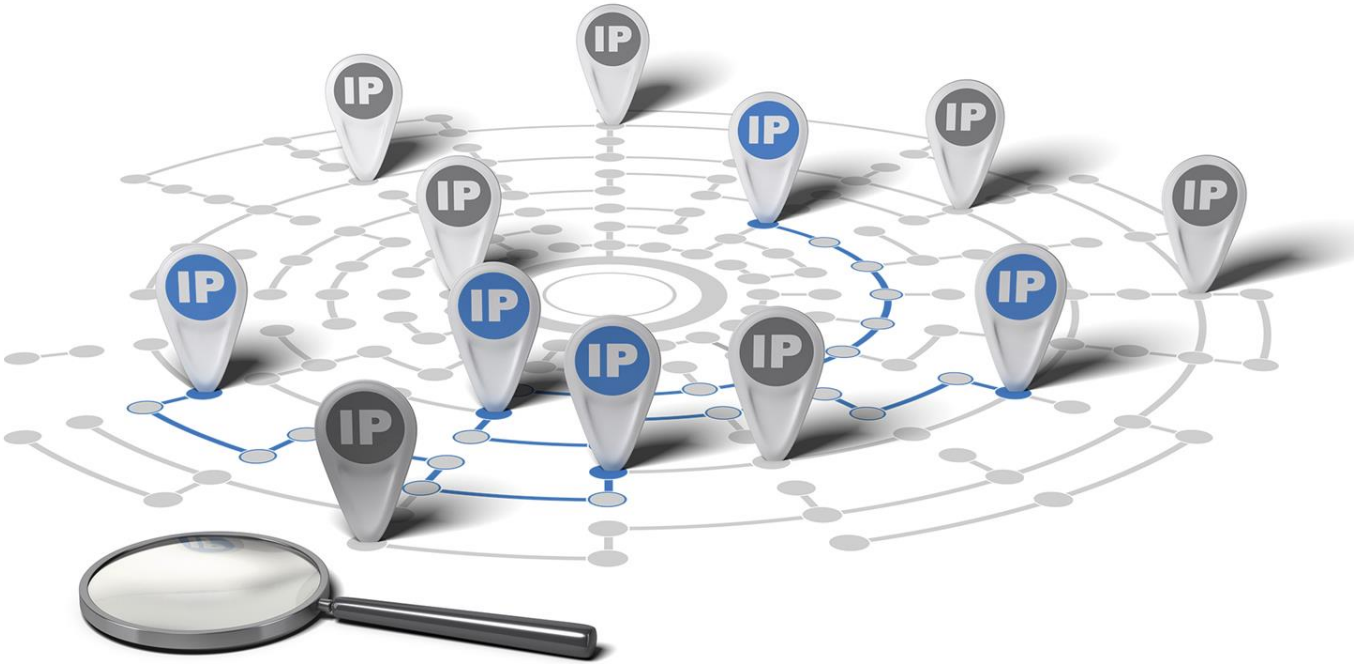
Binary and Network Addresses

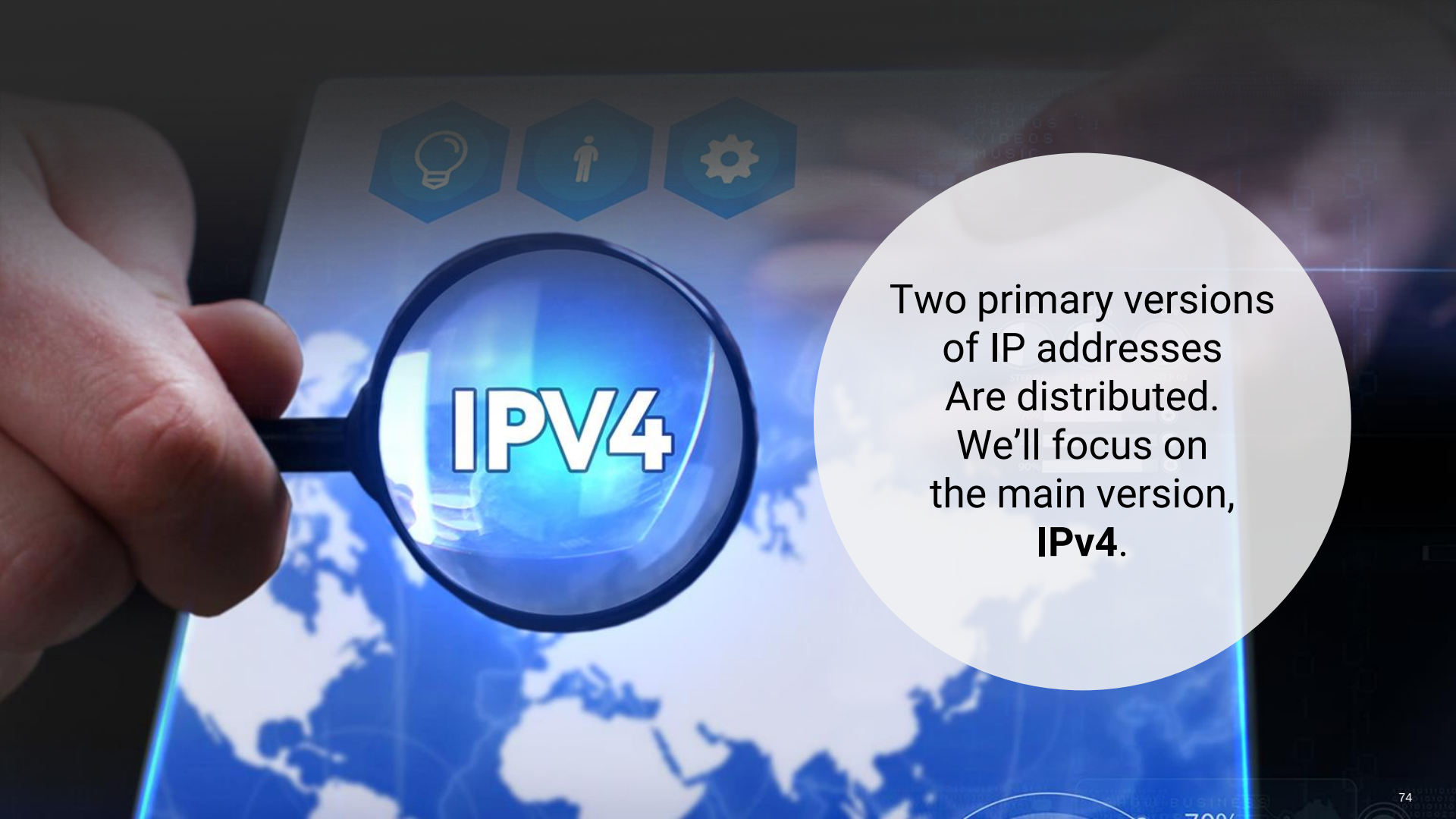
Today, we'll focus on IP addresses.

IP addresses are numerical network addresses associated with a specific device.



Each of our computers has an IP address. Let’s check them at: www.whatsmyip.org.



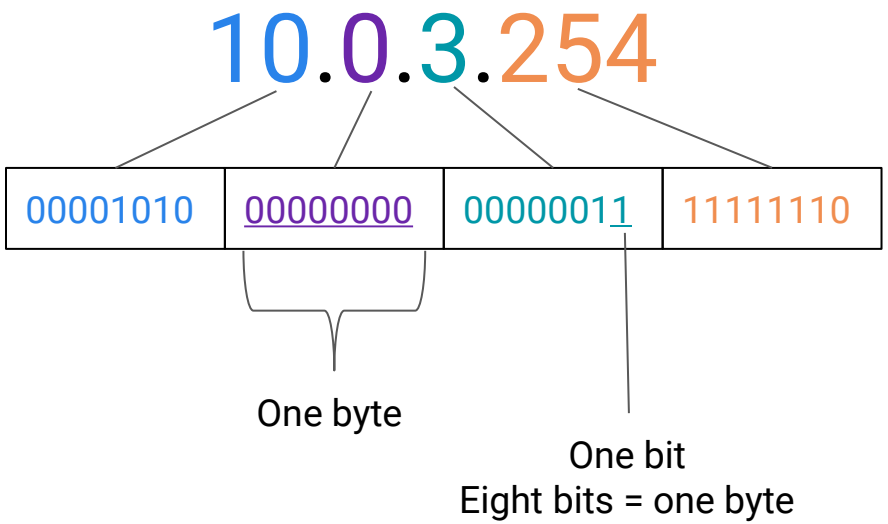


Two primary versions of IP addresses Are distributed. We'll focus on the main version, **IPv4**.

The Anatomy of an IP Address

IPv4 IP addresses are written as four octets separated by decimals.

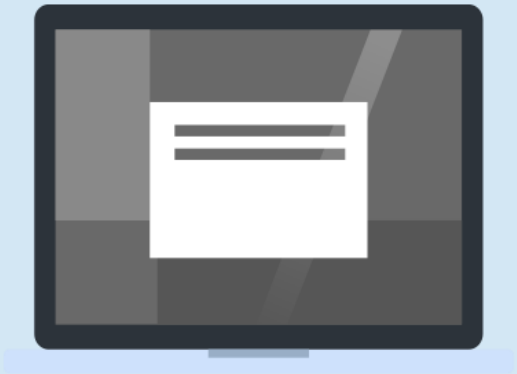
These octets are actually eight binary bits of ones and zeros that are converted to a more interpretable decimal form.



IP Example

10.0.3.254

00001010	00000000	00000011	11111110



What computers read:

`00001010.00000000.00000011.11111110`

What we read:

`10.0.3.254`

Each IP octet can range from zero (`00000000`) to 255 (`11111111`).

Converting IP

Converting IP addresses can be tricky. Lucky for us, there are free online tools to simplify the process.

IP addresses are categorized as public or private.

Public IPs

01

Public IP addresses are addresses that can be accessed over the internet.

- Advantages: Public IPs' resources are accessible over the internet.
- Disadvantages: Not all devices should be accessed over the internet, as this potentially exposes these devices to malicious actors.

02

Public IP addresses are typically assigned out in IP ranges by an Internet Service Provider.

- IP ranges are groups of IP addresses in which the numbers are typically sequential.
- For example, the IP range `108.0.0.1–108.0.0.3` includes:
  - `108.0.0.1`
  - `108.0.0.2`
  - `108.0.0.3`

Private IPs

Private IP addresses are addresses that are not exposed to the internet. Instead, they are typically located within a LAN.

01 Advantages

- Private IP addresses aren't publicly accessible, and therefore more secure.
- Private IPs can be reused, as long as they are in different LANs, since they can't conflict across different networks.

02 Disadvantages

- Private IPs are not directly accessible over the public internet.
- Private IPs are assigned by a network administrator of the LAN they belong to.

Private IPs

Three IPv4 ranges are saved as private IP addresses and used only for private addressing.

Starting IP	Ending IP	IP Addresses Available
10.0.0.0	10.255.255.255	16,777,216
172.16.0.0	172.31.255.255	1,048,576
192.168.0.0	192.168.255.255	65,536

Subnetting

IP addresses
are assigned
manually by the user
or organization that manages
their local network.

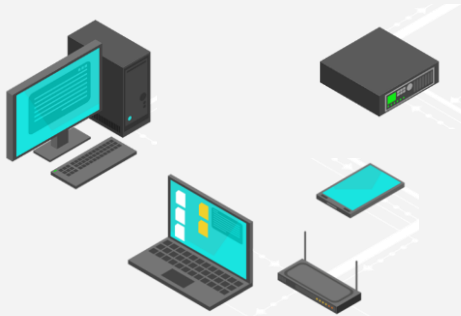
But how do organizations decide
what IP addresses
are assigned?

Subnetting

Organizations will often group their devices together on a network for organizational and efficiency reasons. For example:

An organization would group together servers designated for Finance, and servers designated for M

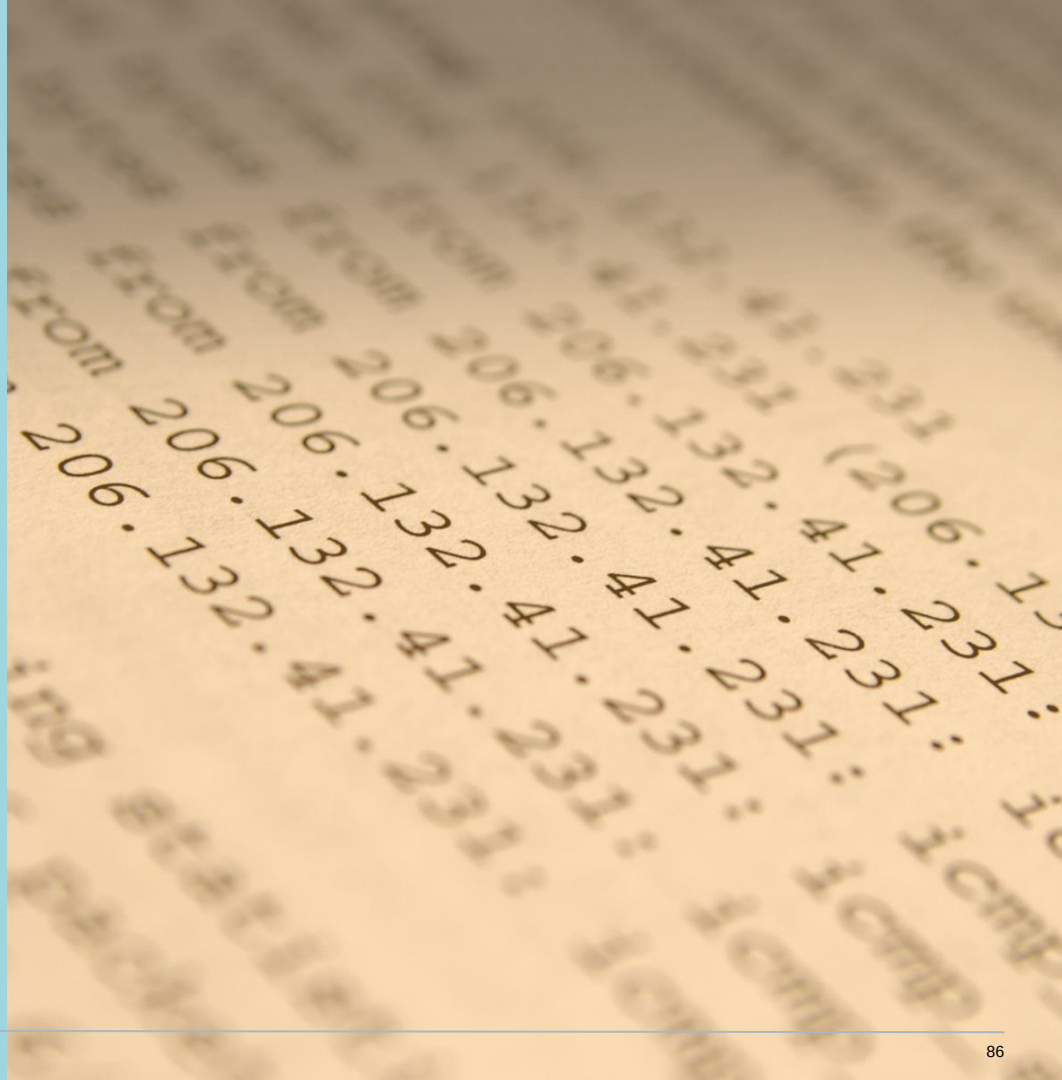
Organizations are typically provided a range of IP addresses that they will distribute across departments and devices.



Subnetting

This process of breaking up an IP address range into smaller, more specific networks of grouped devices is called **subnetting**.

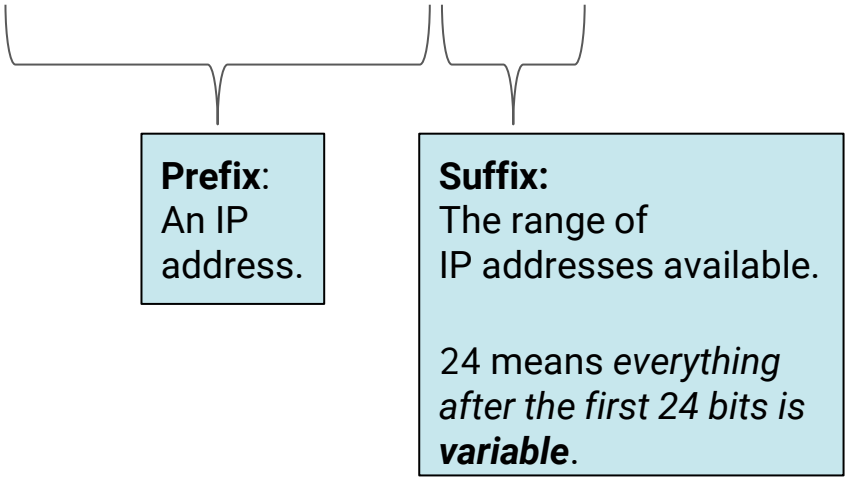
For example: If a company has 100 new IP addresses to distribute, they can assign 50 to the Finance department and 50 to the Marketing department by subnetting their provided IP range.



When we subnet, we don’t have to list and assign IP addresses one by one. Instead, we use a format known as Classless Inter-Domain Routing (CIDR).

CIDRs

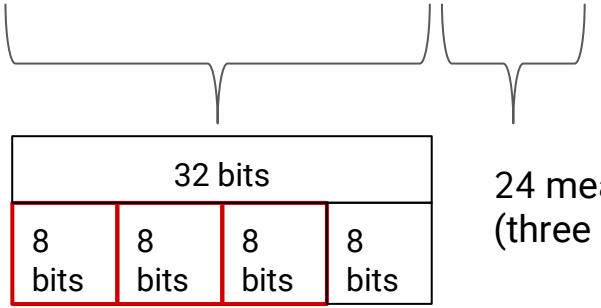
CIDRs are made up of two sets of numbers: An IP address (the prefix) and a range of available IP addresses (the suffix).



CIDRs

CIDRs are made up of two sets of numbers: An IP address and a range of available IP addresses.

192.243.3.0 /24

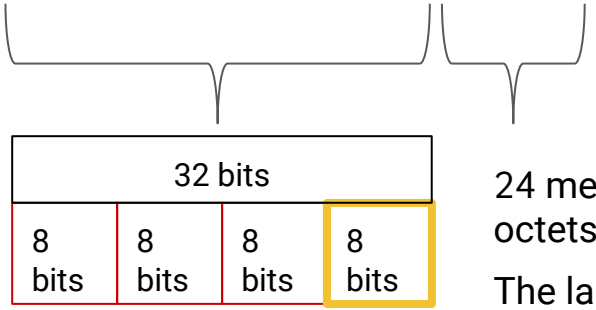


24 means the first 24 bits (three octets) are **static.**

CIDRs

CIDRs are comprised of two sets of numbers: An IP address and a range of IP addresses available.

192.243.3.0 /24



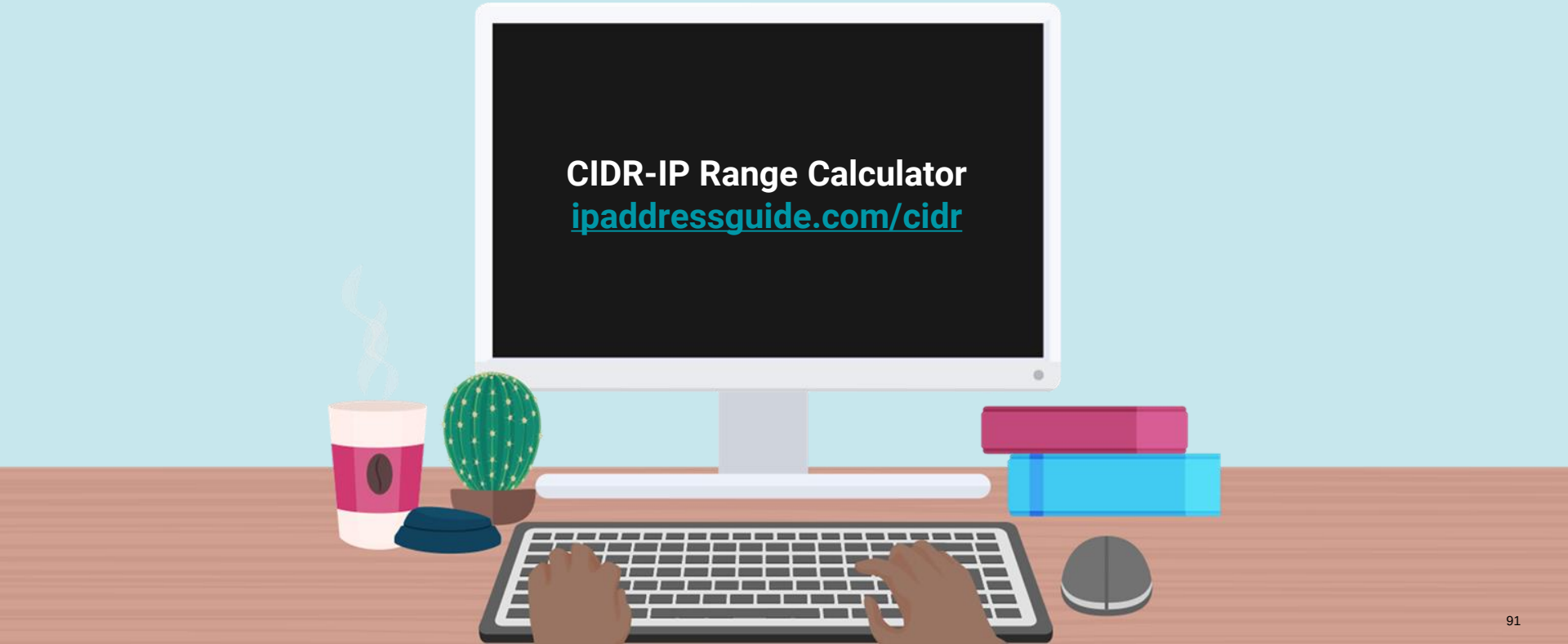
24 means the first 24 bits (three octets) are **static**.

The last 8 bits (`.0`) is **variable**.

- The range of each octet is `0–255`.
- There are 256 available IP addresses in the range `192.243.3.0/24`.

Range Calculator

We can use online tools to easily calculate an IP address range.



MAC Address

Another important network address utilized **within a LAN** is the Media Access Control Address (MAC address).

- MAC addresses are connected to network adapters on a computer and can’t be changed.
- A MAC address is a string of six sets of alphanumeric characters, separated by colons.
- MAC addresses can also indicate the manufacturer of the network device.

Example: `00:0a:95:9d:68:16`

Activity: Network Addressing

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You must convert binary traffic into an IP address, determine if it is public or private, and compare the IP to a list of Acme’s servers to see which systems the hacker is trying to access.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

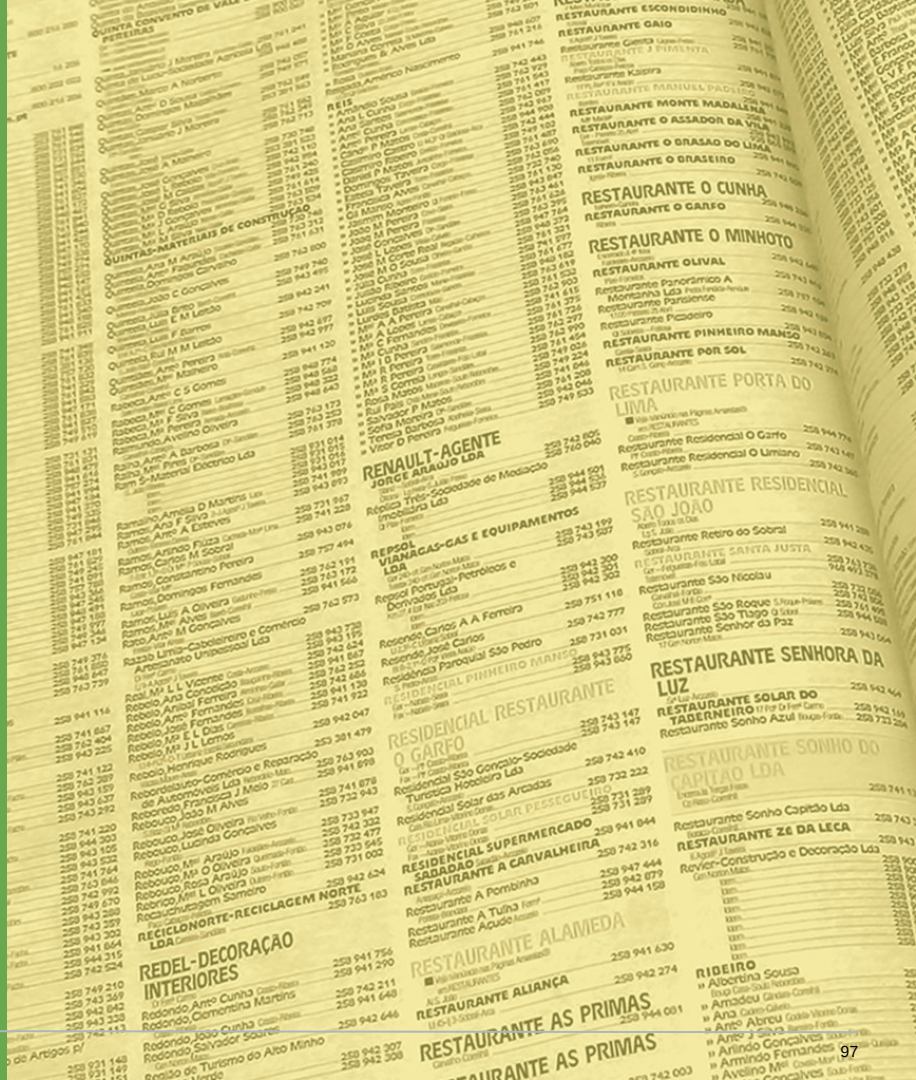
Addresses and the Internet

Now we will look at how accessing data from the internet applies similar network addressing concepts.

Domain Name System (DNS)

Domain Name System allows us to navigate to *facebook.com* instead of having to type *31.13.65.36*.

Using a process called DNS lookup, our browser searches a series of caches to find the IP address associated to the webpage we type.



Lookups and Caches

When a website is entered in a browser, the browser will check DNS caches to see if they already have the DNS translation of the domain’s IP address stored.

Layers of Cache

The caches are searched in an ascending order of scope, starting at your browser's DNS cache and ending, if necessary, at the top-level domain's DNS cache.

1. Browser's cache.

2. The operating system's cache, stored in the hosts file.

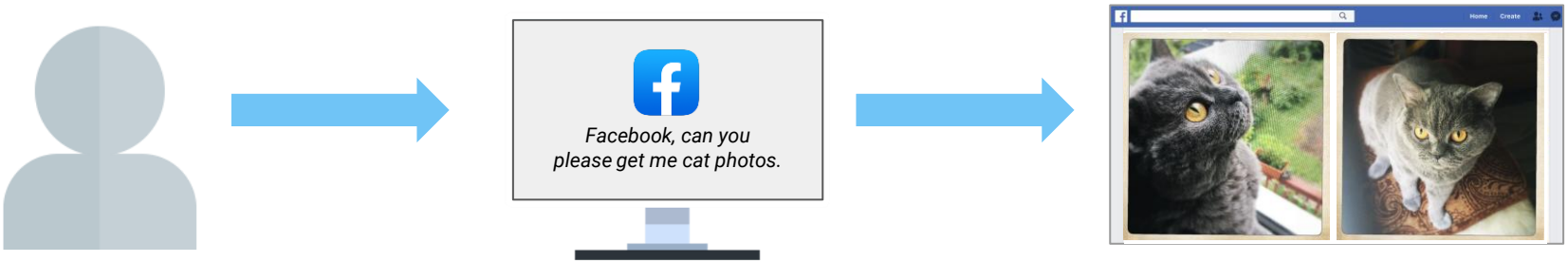
3. Internet Service Provider's (ISP) cache.

4. Finally, the top-level domain's (TLD) cache.

URLs

A domain is the website we access for resources. The resources we're requesting are typically at a specific location within that domain.

For example: If we are viewing a picture from Facebook, the picture likely isn't located at the URL *www.facebook.com*. It is likely at a specific location, such as *www.facebook.com/photos/catpicture.jpg*.



URLs

This resource is located in the URL (Uniform Resource Locator).

A URL is the full address of a resource on the internet.

Similar to file structures, URLs have a syntax indicating where to obtain the specific resource being requested.

The syntax is: `[scheme]://[subdomain].[domain].[TLD][/path/][filename]`

Break Down URL Syntax

https://www.facebook.com/photos/catpicture.jpg

https (*Hypertext Transfer Protocol*) is a scheme indicating a file on the internet.

www is a subdomain of facebook.com.

facebook is the primary domain.

.com is the TLD, or top-level domain.

/photos/is the path where the resource is located.

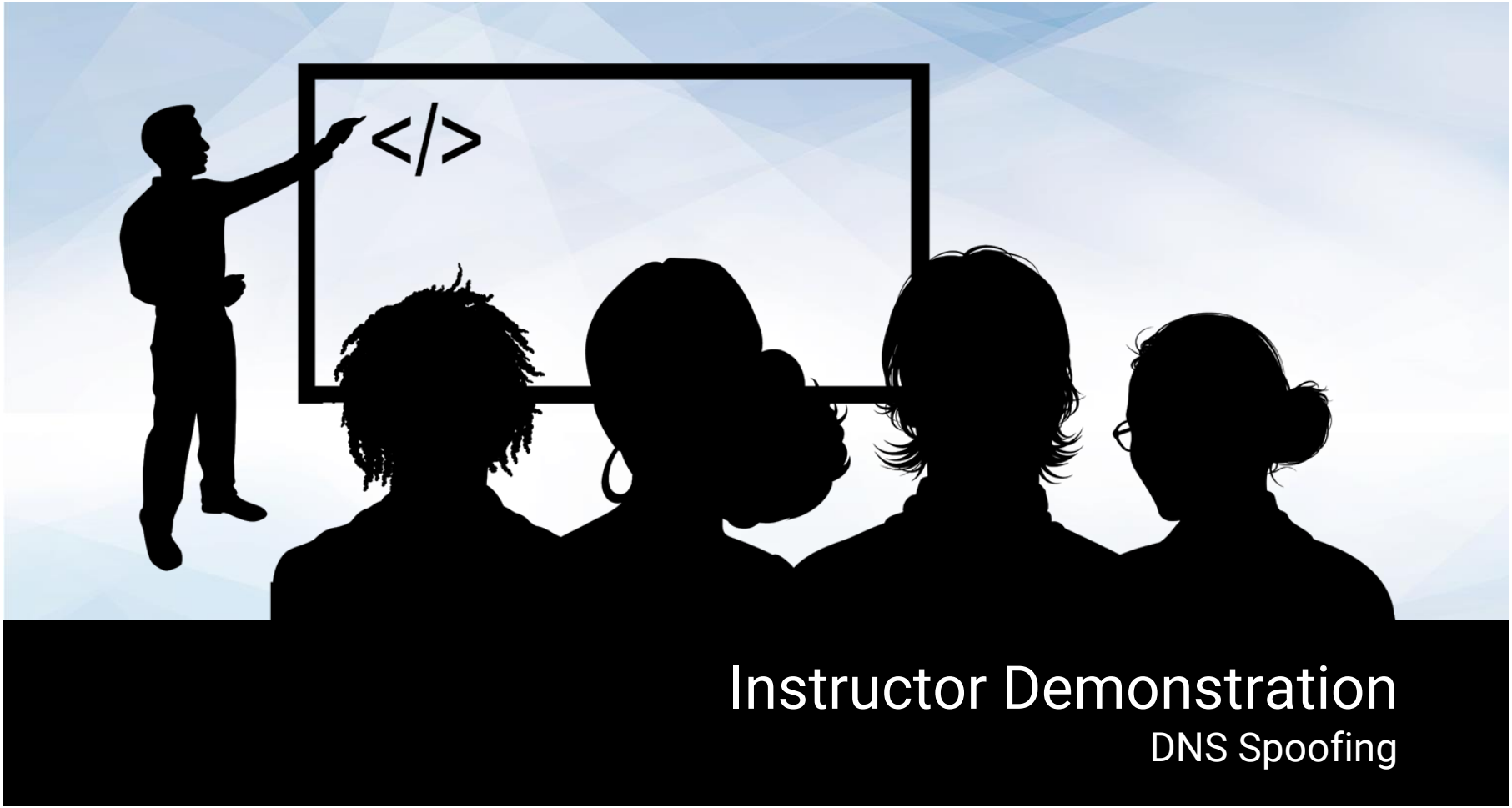
catpicture.jpg is the resource or file being requested.

DNS, URLs, and Security

If a hacker is able to manipulate the DNS cache, they can exploit a user's request and return a domain or resource that wasn't originally requested. This is known as **DNS cache poisoning,** or **DNS spoofing**.

For example:

- A hacker owns a malicious site located at the IP `137.74.187.102`.
- The hacker accesses your hosts file DNS cache and updates a record that makes browser requests for facebook.com go instead to 137.74.187.102.
- Now, every time you go to facebook.com, you are redirected to the hacker's malicious website.



Instructor Demonstration

DNS Spoofing

Activity: DNS Spoofing

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You must create a DNS spoof record that will redirect any hacker trying to visit www.acmetradesecrets.com.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Questions?